21 世纪高等职业教育计算机系列规划教材

网络服务的配置与管理项目实践教程

——基于 Windows Server 2008 平台

齐跃斗　主　编

樊成立　王麟阁　刘庆瑜　副主编

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书以微软公司最新版网络操作系统 Windows Server 2008 为平台，将企业网络信息化建设中常用的网络应用服务所涉及的知识和技能抽象为 9 个具体教学项目，最后以一个完整的企业内部网络设计综合实训项目予以整合。全书采用任务需求式教材编写风格，通过企业案例导入对知识的阐述，以工作任务的实现过程为线索逐一展现学习内容。本书遵循高职教育的“必须、够用”原则，内容编排由浅入深、循序渐进，是一个教、学、做、练相结合的项目实践教材。

本书可作为高职高专院校网络工程、网络管理、计算机应用等专业的教材，也可以作为网络管理、维护人员和技术支持人员快速掌握微软网络技术的必备参考书。为方便教学，本书配有电子教案等参考资料。

图书在版编目（CIP）数据

网络服务的配置与管理项目实践教程：基于 Windows Server 2008 平台/齐跃斗主编．—北京：电子工业出版社，2010.11
（21 世纪高等职业教育计算机系列规划教材）
ISBN 978-7-121-12140-1

Ⅰ．①网…　Ⅱ．①齐…　Ⅲ．①服务器－操作系统（软件），Windows Server 2008－高等学校：技术学校－教材　Ⅳ．①TP316.86

中国版本图书馆 CIP 数据核字（2010）第 211191 号

策划编辑：徐建军
责任编辑：徐　磊
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：14　字数：358.4 千字
印　　次：2010 年 11 月第 1 次印刷
印　　数：3 000 册　　定价：26.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

微软的服务器操作系统是当今主流的网络操作系统，其最新版本的 Windows Server 2008 是专为强化下一代网络、应用程序和 Web 服务的功能而设计的。它在安全性、灵活性、移动性和可靠性等方面都得到了进一步的提高，是有史以来最先进的 Windows Server 操作系统。

本书从 Windows Server 2008 构建网络应用服务的需要出发，较全面地介绍了基于 Windows Server 2008 产品中各种常用的服务器角色，以及它们的搭建、配置与管理方法，如 DNS 服务、DHCP 服务、Web 服务、FTP 服务、系统更新服务、认证服务、VPN 服务和终端服务。全书结构清晰，说明详细，操作以图解导引，便于读者学习和使用。

本书特色思路：

- 本书遵循高职教育的“必须、够用”原则，内容编排由浅入深、循序渐进，突出教学内容的针对性和实用性，体现所对应岗位的能力和技能要求，是一个教、学、做、练相结合的项目实践教材。
- 本书的结构立意新颖，编写思想体现了高职教育的教改方向，即面向工作过程，基于项目驱动，注重技能技巧培养，有利于提高教学效果。
- 本书的编写风格是以企业真实项目为引例导入，以案例的实现过程为主线构造教材结构。每个项目单元（章节）配以知识点、技能点、学习目标等，帮助学生掌握学习方向，引导其学习过程，并配以必要的项目案例实践题和思考题，帮助学生反思学习过程、检验学习效果，使之既有任务操作过程的详尽描述，又有新的任务供学生练习、提高和探索。
- 本书在组织方式上，以项目为教材组织的基本单位。全书将企业网络信息化建设中常用的网络应用服务所涉及到的知识和技能抽象为 9 个具体教学项目并分别实现。以微软公司最新的 Windows Server 2008 操作系统作为载体，实现了该环境下各种常用服务器角色的搭建、配置与管理，最后通过一个完整的案例，将本教材的全部内容整合在一起，要求学生根据要求独立完成企业网络服务系统的建设过程。为帮助学生完成项目，本书详细描述了企业网络建设项目的需求，并针对需求提供了详细的解决方案。为便于项目的具体实施和结果验证，还给出了详尽的测试方案。

本书在结构上采用了 PBL（基于问题的学习方法）设计方法，每个应用服务均以设问提出，以为什么使用该服务功能作为引例，引领读者带着问题读下去，改变了以往平铺直叙、单纯讲述知识点的方法。通过引例，学生不仅能知道该服务功能的作用，而且也能认识到该服务功能在企业信息化网络管理中的意义，增强了读者的学习兴趣，明确了读者学习的目的。

本书由齐跃斗任主编，樊成立、王麟阁、刘庆瑜任副主编。作者均为教学一线的资深教师，均有数年的企业网络技术实践经历。齐跃斗负责全书大纲的编写，项目 2、6、8 的编写，以及全书的修订、统稿工作；樊成立负责项目 7、9 的编写及部分章节的修改；王麟阁负责项目 4、10 的编写；刘庆瑜负责项目 1、3、5 的编写；金珏负责项目 6 中部分内容的编写；贺建伟、慈艳柯、龚俊、张文婷、俞文洋等参与了本书案例设计、书稿校对和 PPT 制作等工作，本书在撰写过程中得到了各方面的大力支持，在此一并表示感谢。

为了方便教师教学，本书配有电子教学课件，请有此需要的教师登录华信教育资源网（www.hxedu.com.cn）免费注册后进行下载，有问题时请在网站留言板留言或与电子工业出版社联系（hxedu@phei.com.cn），也可以直接与作者联系（QYD310@yahoo.com.cn）。

由于对项目式教学法正处于经验积累和改进的过程中，加之编者水平有限、时间仓促，书中难免存在疏漏和不足，希望同行专家和读者能给予批评和指正。

编　者

目　录

项目 1　Windows Server 2008 的网络功能及网络体系架构

基于 IP 协议的因特网，目前已经发展成为当今世界上规模最大、拥有用户最多、资源最广泛的通信网络。IP 协议也因此成为事实上的业界标准，以 IP 协议为基础的网络已经成为通信网络的主流。

本项目将就 IP 协议关于 IP 地址这部分内容，进行简要的阐述。

知识点、技能点

- 了解 IP 地址的结构，并明确在企业中如何分配 IP 地址
- 掌握子网和子网掩码的概念
- 按需求创建子网
- 掌握子网掩码的计算方法，通过子网掩码进行子网的划分

1.1　引例：为什么使用 IP 地址（WHY）

为什么使用 IP 地址？因为 IP 地址是用来标识网络中的一个通信实体的，如一台主机，或者是路由器的某一个端口。而在基于 IP 协议的网络中传输的数据包，也都必须使用 IP 地址来进行标识。

任何一个 IP 地址都是由两部分组成的：网络 ID 和主机 ID。这与现实中的地址组成是类似的，当 IP 数据包在网络上传输的时候，先根据网络 ID 找到目的计算机所处的网络，然后根据主机 ID 在本地网络内将数据包发送给目的计算机。如果以寄普通邮件到学校为例，邮递员一般不是把信直接寄给收件人，而是把收信地址作为两个部分，先把邮件寄到学校的门卫（相当于网络 ID），然后再由学校门卫交给收件人（相当于主机 ID）。

1.2　案例：子网划分

1.2.1　工作情景描述

你是一个公司的网络管理员，目前有 5 个部门 A 至 E。其中，A 部门有 10 台 PC，B 部门有 20 台 PC，C 部门有 30 台 PC，D 部门有 15 台 PC，E 部门有 20 台 PC，然后 CIO 分配了一个总的网段 192.168.2.0/24 给你。作为管理员，你的任务是为每个部门划分单独的网段，你该怎样做呢？

1.2.2　案例分析

在本项目中，你需要满足领导的要求，为 5 个部门分配 IP 地址。并且，只能用 192.168.2.0/24 这个网段。要划分子网，必须制定每一个子网的掩码规划，换句话说，就是要确定每一个子网能容纳的最多的主机数。显然，应该以这几个部门中拥有主机数量最多的部门为准。在本例中，C 部门有 30 台主机，那么子网划分时必须满足至少能容纳 30 台主机。

1.2.3　相关知识

1．OSI 模型

OSI 模型，即开放式通信系统互连参考模型（Open System Interconnection Reference Model），是国际标准化组织（ISO）提出的一个试图使各种计算机在世界范围内互连为网络的标准框架。

OSI 是一个开放性的通行系统互连参考模型，它是一个定义得非常好的协议规范。OSI 模型有 7 层结构，每层都可以有几个子层。下面简单介绍一下这 7 层及其功能。

OSI 的 7 层从上到下如表 1-1 所示（顺序记忆方法为“All People Seems To Need Data Process”）。

表 1-1　OSI 的 7 层及记忆方法

层次	各层名称	英文记忆
第 7 层	应用层（Application Layer）	All
第 6 层	表示层（Presentation Layer）	People
第 5 层	会话层（Session Layer）	Seems
第 4 层	传输层（Transport Layer）	To
第 3 层	网络层（Network Layer）	Need
第 2 层	数据链路层（Data Link Layer）	Data
第 1 层	物理层（Physical Layer）	Process

其中高层，即 7、6、5、4 层，定义了应用程序的功能；下面 3 层，即 3、2、1 层，主要面向通过网络的端到端的数据流。下面介绍一下这 7 层的功能。

（1）应用层：与其他计算机进行通信的一个应用，它是对应应用程序的通信服务的。例如，一个没有通信功能的字处理程序就不能执行通信的代码，从事字处理工作的程序员可能不会关心 OSI 的第 7 层。但是，如果添加了一个传输文件的选项，那么字处理器的程序员就需要实现 OSI 的第 7 层了。示例，Telnet、HTTP、FTP、WWW、NFS、SMTP 等。

（2）表示层：这一层的主要功能是定义数据格式及加密。例如，FTP 允许你选择以二进制或 ASCII 格式传输。如果选择二进制，那么发送方和接收方不改变文件的内容。如果选择 ASCII 格式，发送方将把文本从发送方的字符集转换成标准的 ASCII 后发送数据，接收方会将标准的 ASCII 转换成接收方计算机的字符集。示例，加密、ASCII 等。

（3）会话层：它定义了如何开始、控制和结束一个会话，包括对多个双向会话的控制和管理，以便在只完成连续消息的一部分时可以通知应用，从而使表示层看到的数据是连续的。在某些情况下，如果表示层收到了所有的数据，则用数据代表表示层。示例，RPC、SQL 等。

（4）传输层：这层的功能包括是选择差错恢复协议还是无差错恢复协议，以及在同一主机上对不同应用的数据流的输入进行复用，还包括对收到的顺序不对的数据包的重新排序功能。示例，TCP、UDP、SPX。

（5）网络层：这层对端到端的包传输进行定义，它定义了能够标识所有结点的逻辑地址，还定义了路由实现的方式和学习的方式。为了适应最大传输单元长度小于包长度的传输介质，网络层还定义了如何将一个包分解成更小的包的分段方法。示例，IP、IPX 等。

（6）数据链路层：它定义了在单个链路上如何传输数据。这些协议与被讨论的各种介质有

关。示例，ATM、FDDI 等。

（7）物理层：OSI 的物理层规范是有关传输介质的特性标准，这些规范通常也参考了其他组织制定的标准。连接头、针、针的使用、电流、编码及光调制等都属于各种物理层规范中的内容。物理层常用多个规范完成对所有细节的定义。示例，RJ45、802.3 等。

OSI 分层的优点如下。

- 人们可以很容易地讨论和学习协议的规范细节。
- 层间的标准接口方便了工程模块化。
- 创建了一个更好的互连环境。
- 降低了复杂度，使程序更容易修改，产品开发的速度更快。
- 每层利用紧邻的下层服务，更容易记住各层的功能。

OSI 是一个定义良好的协议规范集，并有许多可选部分能完成类似的任务。

它定义了开放系统的层次结构、层次之间的相互关系，以及各层所包括的可能的任务。它是作为一个框架来协调和组织各层所提供的服务的。

OSI 参考模型并没有提供一个可以实现的方法，而是描述了一些概念，用来协调进程间通信标准的制定，即 OSI 参考模型并不是一个标准，而是一个在制定标准时所使用的概念性框架。

2．TCP/IP 参考模型

TCP/IP 协议并不完全符合 OSI 的 7 层参考模型。传统的开放式系统互连参考模型，是一种通信协议的 7 层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这 7 层分别是物理层、数据链路层、网路层、传输层、会话层、表示层和应用层。而 TCP/IP 通信协议采用了 4 层的层级结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。这 4 层分别如下。

- 应用层：应用程序间沟通的层，如简单电子邮件传输（SMTP）、文件传输协议（FTP）、网络远程访问协议（Telnet）等。
- 传输层：在此层中，它提供了节点间的数据传送服务，如传输控制协议（TCP）、用户数据报协议（UDP）等。TCP 和 UDP 给数据包加入传输数据并把它传输到下一层中，这一层负责传送数据，并且确定数据已被送达并接收。
- 网络层：负责提供基本的数据封包传送功能，让每一块数据包都能够到达目的主机（但不检查是否被正确接收），如网际协议（IP）。
- 网络接口层：对实际的网络媒体的管理，定义如何使用实际网络（如 Ethernet、Serial Line 等）来传送数据。

OSI 与 TCP/IP 的对应关系如表 1-2 所示。

表 1-2　OSI 与 TCP/IP 对应关系

OSI 模型	TCP/IP 模型
应用层	应用层
表示层	
会话层	
传输层	传输层
网络层	网络层
数据链路层	网络接口层
物理层	

1）网际协议 IP

Internet 上使用的一个关键的底层协议是网际协议，通常称 IP 协议。我们利用一个共同遵守的通信协议，使 Internet 成为一个允许连接不同类型的计算机和不同操作系统的网络。要使两台计算机彼此之间进行通信，必须使两台计算机使用同一种“语言”。通信协议正像两台计算机交换信息所使用的共同语言一样，它规定了通信双方在通信中所应共同遵守的约定。

计算机的通信协议精确地定义了计算机在彼此通信过程中的所有细节。例如，每台计算机发送的信息格式和含义，在什么情况下应发送规定的特殊信息，以及接收方的计算机应做出哪些应答，等等。

网际协议 IP 提供了能适应各种各样网络硬件的灵活性，对底层网络硬件几乎没有任何要求，任何一个网络只要可以从一个地点向另一个地点传送二进制数据，就可以使用 IP 协议加入 Internet。

如果希望能在 Internet 上进行交流和通信，则每台连上 Internet 的计算机都必须遵守 IP 协议。为此使用 Internet 的每台计算机都必须运行 IP 软件，以便时刻准备发送或接收信息。

IP 协议对于网络通信有着重要的意义。网络中的计算机通过安装 IP 软件，使许许多多的局域网络构成了一个庞大而又严密的通信系统，从而使 Internet 看起来好像是真实存在的，但实际上它是一种并不存在的虚拟网络，只不过是利用 IP 协议把全世界上所有愿意接入 Internet 的计算机局域网络连接起来，使得它们彼此之间都能够通信而已。

2）传输控制协议 TCP

尽管计算机通过安装 IP 软件，保证了计算机之间可以发送和接收资料，但 IP 协议还不能解决资料分组在传输过程中可能出现的问题。因此，若要解决可能出现的问题，连上 Internet 的计算机还需要安装 TCP 协议来提供可靠的且无差错的通信服务。

TCP 协议被称为一种端对端协议，这是因为它对两台计算机之间的连接起了重要作用。当一台计算机需要与另一台远程计算机连接时，TCP 协议会让它们建立一个连接、发送和接收资料，以及终止连接。

传输控制协议 TCP 利用重发技术和拥塞控制机制，向应用程序提供可靠的通信连接，使它能够自动适应网上的各种变化。即使在 Internet 暂时出现堵塞的情况下，TCP 也能够保证通信的可靠。

众所周知，Internet 是一个庞大的国际性网络，网络上的拥挤和空闲时间总是交替不定的，加上传送的距离也远近不同，所以传输资料所用时间也会变化不定。TCP 协议具有自动调整“超时值”的功能，能很好地适应 Internet 上各种各样的变化，确保传输数值的正确。

因此，从上面我们可以了解到，IP 协议只保证计算机能发送和接收分组资料，而 TCP 协议则可提供一个可靠的、可流控的、全双工的信息流传输服务。

综上所述，虽然 IP 和 TCP 这两个协议的功能不尽相同，也可以分开单独使用，但它们是在同一时期作为一个协议来设计的，并且在功能上也是互补的。只有两者的结合，才能保证 Internet 在复杂的环境下正常运行。凡是要连接到 Internet 的计算机，都必须同时安装和使用这两个协议，因此在实际中常把这两个协议统称为 TCP/IP 协议。

3．IP 地址分类

目前，IP 地址使用 32 位二进制地址格式，为方便记忆，通常使用以点号划分的十进制数来表示，如 202.112.14.1，每个十进制数字的范围是 0～255，如果使用二进制数进行表示正好是 8 位二进制数字。

为了给不同规模的网络提供必要的灵活性，IP 地址空间被划分为 5 个不同的地址类别，其中 A、B、C 3 类最为常用。各类 IP 地址的网络 ID 和主机 ID 字段情况如表 1-3 所示。

表 1-3　网络 ID 和主机 ID 字段情况表

IP 地址类型	IP 地址	网络 ID	主机 ID
A 类	a.b.c.d	a	b.c.d
B 类	a.b.c.d	a.b	c.d
C 类	a.b.c.d	a.b.c	d

1）A 类地址

A 类地址第 1 个字节（8 位二进制数）为网络地址，其他 3 个字节（24 位二进制数）为主机地址。另外，第 1 个字节的最高位固定为 0。A 类地址的网络地址范围是$(00000001)_2$～$(01111111)_2$，即 1～127，所以 A 类 IP 地址范围是 1.0.0.1～126.255.255.254。子网掩码使用 255.0.0.0。

对于每个网络容纳的主机数，我们可以使用公式 2^n-2 来进行计算，这里要减 2，是因为 IP 地址如果主机 ID 为 0，一般用来表示一个网络；如果主机 ID 为二进制的全 1（二进制数 11111111 即为十进制数 255）则表示广播地址，所以可以用来表示主机的主机 ID 数量应当减去 2 个。因此，每个 A 类网络可容纳的主机数量为 $2^{24}-2=16\ 777\ 214$ 台。

Internet 有 126 个可用的 A 类网络地址。A 类地址适用于有大量主机的大型网络。

A 类地址中的私有地址和保留地址如下。

10.0.0.0～10.255.255.255 是私有地址（所谓的私有地址就是在因特网上不使用，而被用在局域网络中的地址，下同）。

127.0.0.0～127.255.255.255 是保留地址，用做循环测试。

0.0.0.0～0.255.255.255 也是保留地址，用做表示所有的 IP 地址。

2）B 类地址

B 类地址第 1、2 字节（16 位二进制数）为网络地址，其他 2 个字节（16 位二进制数）为主机地址。另外，第 1 个字节的最高位固定为 10。B 类地址的网络地址范围是$(10000001)_2$～$(10111111)_2$，即 128～191，所以 B 类 IP 地址范围是 128.0.0.1～191.255.255.254。子网掩码使用 255.255.0.0。

每个 B 类网络可容纳的主机数量为 $2^{16}-2=65\ 534$ 台。

Internet 有 $2^{14}-2=16\ 382$ 个 B 类网络地址。

B 类地址的私有地址和保留地址如下。

172.16.0.0～172.31.255.255 是私有地址。

169.254.0.0～169.254.255.255 是保留地址。如果你的 IP 地址是自动获取 IP 地址的，而你在网络上又没有找到可用的 DHCP 服务器，这时你将会从 169.254.0.0～169.254.255.255 中临时获得一个 IP 地址。

3）C 类地址

C 类地址第 1、2、3 字节（24 位二进制数）为网络地址，最后 1 个字节（8 位二进制数）为主机地址。另外，第 1 个字节的最高位固定为 110。C 类地址的网络地址范围是$(11000001)_2$～$(11011111)_2$，即 192～223，所以 C 类 IP 地址范围是 192.0.0.1 ～223.255.255.254。子网掩码使用 255.255.255.0。

每个 C 类网络可容纳的主机数量为 $2^8-2=254$ 台。

Internet 有 2 097 152 个 C 类网络地址。

C 类地址中的私有地址为 192.168.0.0～192.168.255.255。

4．子网划分

1）子网掩码

子网掩码是一个 32 位地址，用于屏蔽 IP 地址的一部分以区别网络标识和主机标识，并说明该 IP 地址是在局域网上，还是在远程网上。子网掩码不能单独存在，它必须结合 IP 地址一起使用。子网掩码只有一个作用，就是将某个 IP 地址划分成网络地址和主机地址两部分。

子网掩码的设定必须遵循一定的规则。与 IP 地址相同，子网掩码的长度也是 32 位，左边是网络位，用二进制数字“1”表示；右边是主机位，用二进制数字“0”表示。只有通过子网掩码，才能表明一台主机所在的子网与其他子网的关系，使网络正常工作。

2）子网划分

因为在划分了子网后，IP 地址的网络号是不变的，因此在局域网外部看来，这里仍然只存在一个网络，即网络号所代表的那个网络；但在网络内部却是另外一个景象，因为我们每个子网的子网号是不同的，当用划分子网后的 IP 地址与子网掩码（注意，这里指的子网掩码已经不是默认的子网掩码了，而是自定义的子网掩码，是管理员在经过计算后得出的）做“与”运算时，每个子网将得到不同的子网地址，从而实现对网络的划分。

子网编址技术，即子网划分将会有助于以下问题的解决。

（1）巨大的网络地址管理量：如果你是一个 A 类网络的管理员，你一定会为管理数量庞大的主机而头痛的。

（2）路由器中选路表的急剧膨胀：当路由器与其他路由器交换选路表时，Internet 的负载是很高的，所需的计算量也很高。

（3）IP 地址空间有限并终将枯竭：这是一个至关重要的问题，高速发展的 Internet，使原来的编址方法不能适应，而一些 IP 地址却不能被充分利用，造成了浪费。

因此，在配置局域网或其他网络时，根据需要划分子网是很重要的，有时也是必要的。现在，子网编址技术已经被绝大多数局域网所使用。

1.3　案例实施过程

1．案例分析

在这个项目中，在 CIO 所给定的 192.168.2.0/24 网段中，至少要划分出 5 个网段，以满足 5 个部门的需求，并且按照最大化满足的原则，所划分的网段需要容纳至少 30 台机器。

2．实施过程

（1）在这里，我们要使用到经典的计算公式 $2^n-2\geqslant x$。首先要满足的是主机数，因此 x 就是 30，而 n 是子网掩码中用来表示主机位的位数。因此 $2^n-2\geqslant 30$，得出 $n=5$。

注：如果 x 表示所要划分的子网数，则 n 得出的结果就是子网掩码中表示网络 ID 的位数，即高位为 n 个 1，剩余低位即是主机 ID，即为 0 的个数。

（2）由于 n 表示子网掩码中用来表示主机位的位数，因此子网掩码中最后 5 位为 0，则前 3 位是 1。而项目中已给出的子网掩码是 255.255.255.0，则新的子网掩码应为 255.255.255.11100000，即 255.255.255.224，如表 1-4 所示。

表 1-4　子网掩码计算

原子网掩码	计算后得出的结论	新的子网掩码
255.255.255.00000000	最后 5 位（即低 5 位）是主机 ID，为 0；高 3 位是网络 ID	255.255.255.11100000
255.255.255.0		255.255.255.224

（3）按照新的子网掩码，计算各网段的网络 ID。对于网络 ID 来说，其可变范围是 001～110，用网络 ID 与子网掩码进行 AND（与）操作，即可得出各网段的网段号，如表 1-5 所示。

表 1-5　子网网段计算

网段号	A	B	C	D	E	F
网络 ID	00100000	01000000	01100000	10000000	10100000	11000000
子网掩码	11100000	11100000	11100000	11100000	11100000	11100000
AND 结果（10 进制）	32	64	96	128	160	192

6 个子网的网段地址，如表 1-6 所示。

表 1-6　新的子网 ID

子网 A	子网 B	子网 C	子网 D	子网 E	子网 F
192.168.32.011	192.168.64.0	192.168.96.0	192.168.128.0	192.168.160.0	192.168.192.0

（4）计算各子网的 IP 范围，如表 1-7 所示。

表 1-7　各子网的 IP 信息

子网	二进制子网号	二进制主机号范围	十进制主机号范围	可容纳的主机数	子网地址	广播地址
A	001	00000～11111	.32～.63	30	.32	.63
B	010	00000～11111	.64～.95	30	.64	.95
C	011	00000～11111	.96～.127	30	.96	.127
D	100	00000～11111	.128～.159	30	.128	.159
E	101	00000～11111	.160～.191	30	.160	.191
F	110	00000～11111	.192～.223	30	.192	.223
注意：主机位全 0 代表网络地址，主机位全 1 代表广播地址。						

整理为常用 IP 形式，如表 1-8 所示。

表 1-8　最终子网 IP 信息列表

子网	IP 地址范围	可容纳的主机数	子网地址	广播地址
A	192.168.2.32～192.168.2.63	30	192.168.2.32	192.168.2.63
B	192.168.2.64～192.168.2.95	30	192.168.2.64	192.168.2.95
C	192.168.2.96～192.168.2.127	30	192.168.2.96	192.168.2.127
D	192.168.2.128～192.168.2.159	30	192.168.2.128	192.168.2.159
E	192.168.2.160～192.168.2.192	30	192.168.2.160	192.168.2.191
F	192.168.2.192～192.168.2.223	30	192.168.2.192	192.168.2.223

至此，已经完成了子网划分的任务要求，即 5 个部门需要 IP 地址，并且单个部门最多的计算机数是 30 台。在 CIO 提供的 1 个 C 类网段上，划分了 6 个子网，每个子网能容纳 30 台主机，完全满足这个项目的需求。

本项目提出的需求，经过分析后，需要达到以下目的。

- 需要 5 个网段，来给 5 个部门使用。
- 每个网段内要能容纳下 30 台计算机。
- 每个部门都使用一个 C 类地址是最方便实现的方法，但会造成 IP 地址浪费。
- 公司的 CIO 只给了你一个 C 类地址段。

你需要在以上基础上完成任务。经过子网划分，我们将一个 C 类网络划分为了 6 个小的子网，而且保证了每个子网可以容纳 30 台计算机，满足了项目需求，圆满完成了任务。

1.4　知识能力拓展

1.4.1　利用子网掩码判断机器是否为远程

子网掩码是用来判断任意两台计算机的 IP 地址是否属于同一子网络的根据。最为简单的理解就是两台计算机各自的 IP 地址与子网掩码进行 AND 运算后，如果得出的结果是相同的，则说明这两台计算机是处于同一个子网络上的，可以进行直接的通信。请看以下示例。

以下 IP 地址中，哪些地址不需要通过路由器就可以直接通信，即在同一网段内？

a．10.10.85.24/20　b. 10.10.213.24/20　c. 10.10.3.24/20　d. 10.10.95.24/20

如果只从 IP 来看，这 4 个 IP 地址似乎都是同一个网段，但子网掩码并不是 A 类默认的 8 位，即 255.0.0.0。此时，我们需要通过子网掩码与 IP 的与运算，来确定哪些 IP 是同一网段的。

子网掩码为 20 位，即 11111111.11111111.11110000.00000000，前两段已经是全 1，只有第 3 段不是全 1。因此，我们需要用 IP 地址中的第 3 段与子网掩码中的第 3 段进行与操作，如表 1-9 所示。

表 1-9　计算方法

	a	b	c	d
第 3 段化为二进制	01010101	11010101	0011000	01011111
子网掩码第 3 段	11110000	11110000	11110000	11110000
与运算结果（二进制）	01010000	11010000	00010000	01010000

可以看到，与运算结果中，a 与 d 的结果相同，均为 01010000。也就是说，a 和 d 均属于 10.10.80.0/20 这个网段。因此，a 与 d 的通信不需要通过路由器。

1.4.2　可变长子网掩码——VLSM

VLSM 是一种为节约 IP 地址而创建的不同子网的方法。如果用户使用固定的子网掩码在某一网络中进行子网化，而这个网络的各子网对主机的最大数目有着不同的要求，那么可能会产生浪费大量 IP 地址的情况。通过使用 VLSM，可以给每个子网分配合适数目的 IP 地址，而不是使用固定长度的子网掩码。

VLSM 是如何节约 IP 地址的呢？

子网划分不需要相同大小的子网，所以用户可以通过使用 VLSM 来创建规模大小不同的子网，使每一个子网的规模与每个子网的主机数目达到最佳匹配，从而达到节约 IP 地址的目的。VLSM 使用子网划分将已经被子网化过的网络 ID 再次进行子网化。这个过程可以一直持续下去，直到得到多个唯一的子网 ID，并且这些子网 ID 可以尽可能减少每个子网上的 IP 地址浪费为止。因为所有的子网化过的网络 ID 是唯一的，可以通过对应的子网掩码互相区分。

1．IP 地址浪费的示例

在表 1-10 中，有 7 个子网。

表 1-10　子网数与主机数

子网	1	2	3	4	5	6	7
主机数	2	2	62	97	28	153	4

如果用户使用 24 位固定长度的子网掩码，则会使用 7 个 C 类网段，每个网段中的 IP 地址数为 254，共要使用 7×254=1 778 个 IP 地址，而实际使用的 IP 地址数量只有 2+2+62+97+28+153+4=348 个，浪费了 1 430 个 IP 地址。如果使用 VLSM，可以使这个浪费数量大大减少。

2．VLSM 的使用方法

场景描述：现有网络 ID157.54.0.0/16，需要的配置为如下要求的子网。

- 一个最多带 32 000 台主机的子网。
- 分成 15 个最多各带 2 000 台主机的子网。
- 分成 8 个最多各带 250 台主机的子网。

（1）一个子网带 32 000 台主机的子网划分过程。

为了达到一个子网能容纳 32 000 主机的需求，把网络 ID 157.54.0.0 子网化 1 位，就能产生两个子网 157.54.0.0/17 和 157.54.128.0/17。在这里，32 位子网掩码中，有 17 位作为网络位，剩下的 15 位为主机位，这样子网划分出来，每个子网可以容纳的主机数为 $2^{15}-2=32\ 766$ 台。我们选择低网段号 157.54.0.0/17 作为网络 ID，就可以满足需求了，如表 1-11 所示。

表 1-11　1 个子网带 32 000 台主机

子网号	网络 ID（十进制数）	网络 ID（网络前缀）
1	157.54.0.0，255.255.128.0	157.54.0.0/17

（2）15 个子网各带 2 000 台主机的划分过程。

为了满足 15 个子网各带 2 000 台主机的需求，我们选择已经子网化的网络 ID157.54.128.0/17 来进行再次子网化（157.54.0.0/17 已经在上面被使用）。把经过子网化的网络 ID157.54.128.0/17 再划分出 4 位，就产生了 16 个子网（157.54.128.0/21，157.54.136.0/21～157.54.240.0/21，157.54.248.0/21），每个子网可以容纳的主机数为 2 046 台。经子网化的网络 ID（157.54.128.0/21～157.54.240.0/21）的前 15 位用做网络 ID，则刚好满足需求，具体情况如表 1-12 所示。

表 1-12　15 个子网各带 2 000 台主机

子网号	网络 ID（十进制数）	网络 ID（网络前缀）
1	157.54.128.0，255.255.248.0	157.54.128.0/21
2	157.54.136.0，255.255.248.0	157.54.136.0/21
3	157.54.144.0，　255.255.248.0	157.54.144.0/21
4	157.54.152.0，255.255.248.0	157.54.152.0/21
5	157.54.160.0，255.255.248.0	157.54.160.0/21
6	157.54.168.0，255.255.248.0	157.54.168.0/21
7	157.54.176.0，255.255.248.0	157.54.176.0/21
8	157.54.184.0，255.255.248.0	157.54.184.0/21
9	157.54.192.0，255.255.248.0	157.54.192.0/21
10	157.54.200.0，255.255.248.0	157.54.200.0/21
11	157.54.208.0，255.255.248.0	157.54.208.0/21
12	157.54.216.0，255.255.248.0	157.54.216.0/21
13	157.54.224.0，255.255.248.0	157.54.224.0/21
14	157.54.22.0，255.255.248.0	157.54.22.0/21
15	157.54.240.0，255.255.248.0	157.54.240.0/21

（3）8 个子网各带 250 台主机的划分过程。

为了满足 8 个子网各带 250 台主机的配置要求，把经过子网化的网络 ID157.54.248.0/21 再划分出 3 位，就产生了 8 个子网（157.54.248.0/24，157.54.249.0/24～157.54.254.0/24，157.54.255.0/24）作为网络 ID，则刚好满足需求，如表 1-13 所示。

表 1-13　8 个子网各带 250 台主机

子网号	网络 ID（十进制数）	网络 ID（网络前缀）
1	157.54.248.0，255.255.255.0	157.54.248.0/24
2	157.54.249.0，255.255.255.0	157.54.249.0/24
3	157.54.250.0，255.255.255.0	157.54.250.0/24
4	157.54.251.0，255.255.255.0	157.54.251.0/24
5	157.54.252.0，255.255.255.0	157.54.252.0/24
6	157.54.253.0，255.255.255.0	157.54.253.0/24
7	157.54.254.0，255.255.255.0	157.54.254.0/24
8	157.54.255.0，255.255.255.0	157.54.255.0/24

1.5　项目完成结论

通过完成本项目中的案例，学习了 IP 地址的相关知识，如 OSI 参考模型、TCP/IP 协议层等，掌握了子网掩码的作用，如何判断 IP 地址分类、如何按照要求进行子网划分等知识，并在此基础上学习了可变长子网掩码 VLSM，以满足特殊要求的子网划分。

1.6　练习案例

某公司准备在网络中部署 IP 地址，公司准备使用 192.168.1.0 这个 C 类的 IP 网络，公司每个办公室有 10 台计算机，将来准备扩展为 20 台，而公司目前有 6 个办公室。请确定应该使用怎样的子网掩码。

1.7　课后习题

1．192.168.1.0/24 使用掩码 255.255.255.240 划分子网，其可用子网数为（　　），每个子网内可用主机地址数为（　　）。

A．14　14　　B．16　14

C．254　6　　D．14　62

2．子网掩码为 255.255.0.0，下列哪个 IP 地址不在同一网段中（　　）。

A．172.25.15.201　　B．172.25.16.15

C．172.16.25.16　　D．172.25.201.15

3．B 类地址子网掩码为 255.255.255.248，则每个子网内可用主机地址数为（　　）。

A．10　　B．8

C．6　　D．4

4．对于 C 类 IP 地址，子网掩码为 255.255.255.248，则能提供子网数为（　　）。

A．16　　B．32

C．30　　D．128

5．IP 地址 219.25.23.56 的默认子网掩码有（　　）位。

A．8　　B．16

C．24　　D．32

6．某公司申请到一个 C 类 IP 地址，但要连接 6 个子公司，最大的一个子公司有 26 台算机，每个子公司在一个网段中，则子网掩码应设为（　　）。

A．255.255.255.0　　B．255.255.255.128

C．255.255.255.192　　D．255.255.255.224

7．一台 IP 地址为 10.110.9.113/21 的主机在启动时发出的广播 IP 是（　　）。

A．10.110.9.255　　B．10.110.15.255

C．10.110.255.255　　D．10.255.255.255

8．规划一个 C 类网，需要将网络分为 9 个子网，每个子网最多 15 台主机，（　　）是合适的子网掩码。

A．255.255.224.0　　B．255.255.255.224

C．255.255.255.240　　D．没有合适的子网掩码

项目 2　AD 服务的安装、配置与管理

公司有着严密的组织结构，通过这种组织结构，公司能有效地管理公司的员工。我们能不能像公司管理员工那样管理我们的计算机和计算机用户呢？能。活动目录就是实现这种管理的有效工具。通过本章的学习，你将能够安装活动目录，并通过活动目录来有效地管理公司的每一台计算机和计算机用户。

知识点、技能点

- 掌握域的概念
- 能够建立独立域控制器
- 能够确认域控制器是否安装正常并进行故障排除
- 能够删除活动目录
- 能够创建额外域控制器
- 能够创建子域
- 能够创建森林

2.1　引例：为什么要安装和配置 AD（WHY）

你是公司的网络管理员，公司规模在不断壮大，计算机数目在不断增长，现在有计算机 500 台，计算机用户 600 个。公司有很多共享文件，不同级别和类别的共享文件只能让相应级别和类别的用户读取或者修改……要怎么管理这些计算机、计算机用户和共享文件呢？

我们知道，公司有着严密的组织结构和规章制度，通过这种组织结构和规章制度，公司能有效地管理公司的员工。我们能不能像公司管理员工那样管理我们的计算机和计算机用户，以及其他资源呢？能。活动目录就是实现这种管理的有效工具。

2.2　案例 1：使用域管理公司的网络

2.2.1　工作情景描述

DHYNET 公司的网络规模不断扩大，公司决定采用域模式管理公司的网络。公司有办公室、生产部、销售部、采购部、财务部、人事部和客服部等部门。请为 DHYNET 公司规划并构建域。

2.2.2　案例分析

DHYNET 公司网络暂时没有与其他单位的网络连接，因此域林中只要构建一个域树即可。DHYNET 公司有 7 个下属部门，要构建 7 个子域。当然，也可以为部门的下属单位构建再下一级的子域。域树结构如图 2-1 所示。

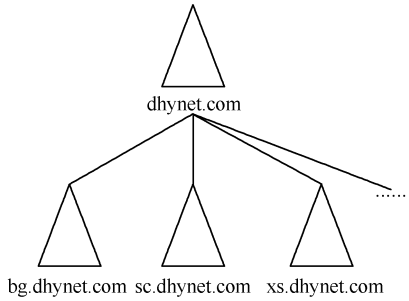

图 2-1　DHYNET 公司域树图

2.2.3　相关知识

1．什么是活动目录

活动目录就是 Active Directory（AD）。Microsoft Active Directory 服务是 Windows 平台的核心组件，Active Directory 存储了有关网络对象的信息，这些对象包括用户、用户组、计算机、域、组织单位（OU）、组、文件、打印机、应用程序、服务器，以及安全策略等。Active Directory 为管理员对这些对象进行组织和管理提供了一种有力的手段。

2．为什么要提供目录服务

对更加强大、透明且高度集成的目录服务的不断需求是由爆炸性增长的网络计算所导致的。随着局域网（LAN）、广域网（WAN）规模与复杂性的不断提高和这些网络不断被连入 Internet，以及应用程序对网络的依赖程度不断增强并不断被链接到协作企业网中的其他系统上，系统对目录服务的需求也日渐增多。基于下列原因，目录服务成为扩展的计算机系统中最重要的部件之一。

- 简化管理。提供对用户、应用程序和设备的单一性、一致性的管理点。
- 加强安全性。向用户提供单一的网络资源登录，为管理员提供强大、一致性的工具以使他们能够管理为内部台式机用户、远程拨号用户，以及外部电子商务客户提供的安全服务。
- 扩展的互操作性。向所有活动目录特性提供基于标准的存取方式及对通用目录的同步支持。

目录服务兼任管理工具和用户工具。随着网络中对象数量的增加，目录服务变得必不可少。目录服务在一个庞大的分布式系统中发挥着网络集线器的作用。基于这些需求，从 Windows 2000 服务器版开始引入了活动目录，即一套用于改进 Windows 网络操作系统管理、安全性和互操作性的完整的目录服务集。

3．活动目录与域控制器有什么关系

安装了活动目录的计算机被称为域控制器。

4．域与工作组的区别是什么

1）“自由”的工作组

工作组（Work Group）就是将不同的计算机按功能分别列入不同的组中，以方便管理。比如，在一个网络内，可能有成百上千台计算机，如果这些计算机不进行分组，都列在“网上邻居”内，可想而知会有多么乱（恐怕网络邻居也会显示“下一页”吧）。为了解决这一问题，

Windows 9x/NT/2000 才引入了“工作组”这个概念，如一所高校，会分为数学系、中文系等，然后数学系的计算机全都列入数学系的工作组中，中文系的计算机全都列入中文系的工作组中……如果你要访问某个系别的资源，就在“网上邻居”里找到那个系的工作组名，双击即可看到那个系别的计算机了。

那么怎样才能加入工作组中呢？其实方法很简单，只需要右击（用鼠标右键单击）Windows 桌面上的“网上邻居”，在弹出的菜单中选择“属性”，单击“标识”，在“计算机名”一栏中输入你想好的名字，在“工作组”一栏中输入你想加入的工作组名称。如果你输入的工作组名称是一个不存在的工作组，那么就相当于新建一个工作组，当然也只有你自己的计算机在里面。不过要注意，计算机名和工作组的长度都不能超过 15 个英文字符，可以输入汉字，但是也不能超过 7 个汉字。“计算机说明”是附加信息，不填也可以，但是最好填。提示需要重新启动，按要求重新启动之后，再进入“网上邻居”，就可以看到你所在工作组的成员了。

同加入工作组相类似，计算机的管理员也可以自由地退出工作组，也可以自由地创建新的工作组。

2）域的管理和设置

打个比方，如果说工作组是“免费的旅店”，那么域（Domain）就是“星级的宾馆”；工作组可以随便出出进进，而域则需要严格控制。“域”的真正含义指的是服务器控制网络上的计算机能否加入的计算机组合，类似于社会组织。一提到组合，势必需要严格控制。所以实行严格的管理对网络安全是非常必要的。在对等网模式下，任何一台计算机只要接入网络，其他机器就都可以访问共享资源，如共享上网等。尽管对等网络上的共享文件可以加访问密码，但是非常容易被破解。在由 Windows 9x 构成的对等网中，数据的传输是非常不安全的。

不过在“域”模式下，至少有一台服务器负责每一台连入网络的计算机和用户的验证工作，相当于一个单位的门卫一样，称为域控制器（Domain Controller，DC）。

域控制器中的 Active Directory 存储了有关网络对象的信息，这些对象包括用户、用户组、计算机、域、组织单位（OU）、组、文件、打印机、应用程序、服务器及安全策略等。当计算机连入网络时，域控制器首先要鉴别这台计算机是否是属于这个域的，用户使用的登录账号是否存在、密码是否正确。如果以上信息有一样不正确，那么域控制器就会拒绝这个用户从这台计算机登录。不能登录，用户就不能访问服务器上有权限保护的资源，他只能以对等网用户的方式访问 Windows 共享出来的资源，这样就在一定程度上保护了网络上的资源。

要把一台计算机加入域，仅仅使它和服务器在网上邻居中能够相互“看”到是远远不够的，必须要由网络管理员进行相应的设置。

5．创建域的条件是什么

- 在 Windows Server 2008 系统中必须安装了 Windows Server 2008 标准版、Windows Server 2008 企业版或者 Windows Server 2008 数据中心版中的任何一种操作系统，但不能是 Windows Server 2008 Web 版。
- 必须有一个静态的 IP，如 192.168.0.1。
- 必须有一个硬盘是 NTFS 格式的，用于放置 SYSVOL 文件夹（微软的建议是全部硬盘都用 NTFS 格式）。
- 安装的时候必须有管理员权限。
- 符合 DNS 规格的 DNS 域名，如 dhynet.com。
- DNS 服务器。

6．什么是域树和域林

域树由多个域组成，这些域共享同一表结构和配置，形成一个连续的名字空间，如图 2-2 所示。所谓连续的名称空间是指子域的名称中包含父域的名称，如 sales.abc.net 包含父域 abc.net 的全部名称，beijing.sales.abc.net 包含它的父域 sales.abc.net 的全部名称。

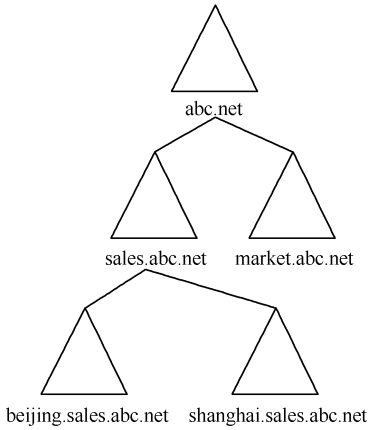

图 2-2　域树

一个或多个域树可以组成一个域林，如图 2-3 所示。域树 abc.net 和域树 dhynet.com 构成了域林。一个域树与另一个域树的名称空间是不连续的。

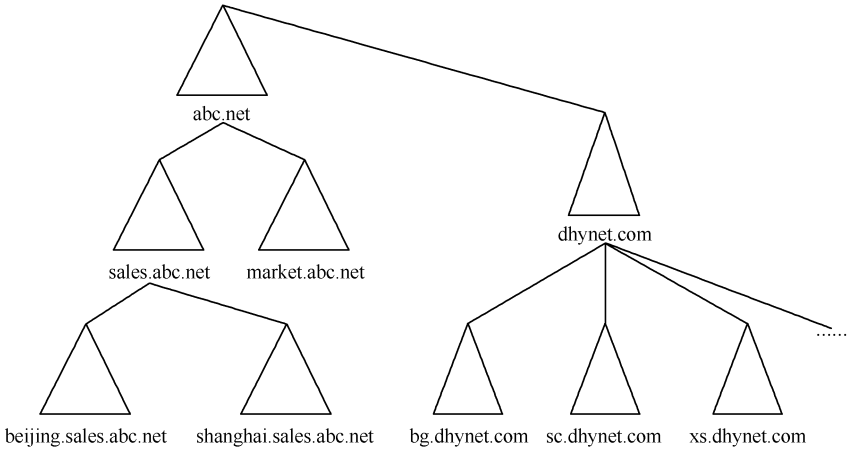

图 2-3　域林

注意：单个域树也构成一个域林。

7．域控制器、成员服务器、独立服务器有什么区别

安装活动目录（AD）的服务器就是域控制器，加入域但没有安装 AD 的服务器是成员服务器，没有加入域的服务器是独立服务器。

2.3　案例 1 实施过程

要为 DHYNET 公司构建域模式的网络，首先要构建独立的域控制器，在这个域控制器中建立域 dhynet.com，为了提高效率和容错，还要构建 dhynet.com 的辅助的额外域控制器，最后构建 dhynet.com 的各个子域，如 bg.dhynet.com。

2.3.1　任务 1：创建网络中的第一台域控制器

在 Windows Server 2008 中，通过采用以下方式启动 Active Directory 域服务安装向导，可以交互式地添加 Active Directory 域控制器服务器角色。

- 可以使用“添加角色向导”。可以采用以下方式访问“添加角色向导”，在服务器管理器（始终可在“管理工具”菜单上或通过通知区域中的图标使用）中，单击“添加角色”。添加角色向导将在服务器上安装和配置 Active Directory 域服务（AD DS）所需的文件，但不会启动实际的 AD DS 安装。完成添加角色向导后，单击启动 Active Directory 域服务安装向导的链接。
- 可以单击“开始”→“运行”，然后输入 dcpromo，就像在以前的 Windows Server 操作系统版本中一样。

下面使用“添加角色向导”来添加域控制器服务器角色。

（1）单击“开始”→“服务器管理器”，打开“服务器管理器”窗口，如图 2-4 所示。

图 2-4　“服务器管理器”窗口

（2）在图 2-4 中单击“添加角色”，打开“添加角色向导”的第一个对话框“开始之前”对话框，如图 2-5 所示。请按照图 2-5 中的要求进行检查，如果你的计算机的 Administrator 账户没有强密码，或者你的计算机没有静态 IP 地址，那么请你单击“取消”，为 Administrator 账户设置强密码，或者为你的计算机设置静态 IP 地址，然后再重新启动“添加角色”向导。

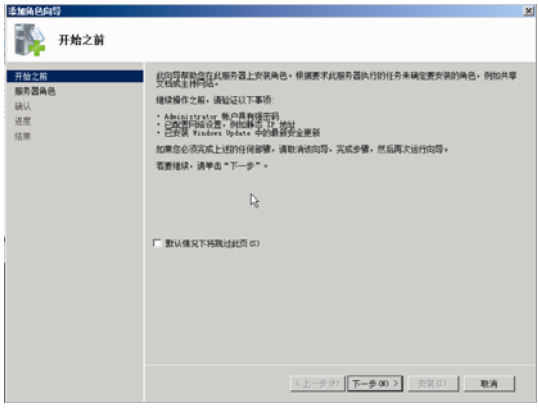

图 2-5　阅读注意事项

（3）在图 2-5 中单击“下一步”按钮，打开“选择服务器角色”对话框，如图 2-6 所示。勾选“Active Directory 域服务”复选框，单击“下一步”按钮。

图 2-6　选择“Active Directory 域服务”

（4）弹出如图 2-7 所示的“Active Directory 域服务”对话框，单击“下一步”按钮。

图 2-7　Active Directory 域服务的说明

（5）出现如图 2-8 所示的“确认安装选择“对话框后，单击“安装”按钮。

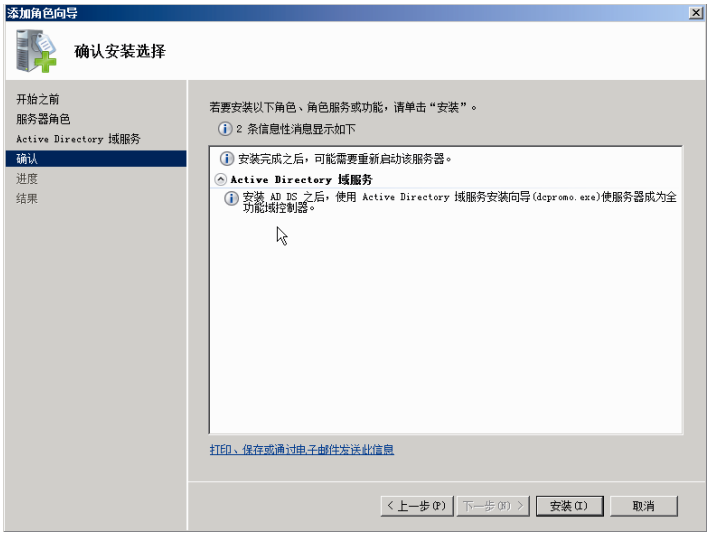

图 2-8　确认安装选择

（6）等待安装完成。完成后显示如图 2-9 所示的“安装结果”对话框。在该对话框中单击“关闭”按钮，将启动 Active Directory 域服务安装向导。

图 2-9　安装完成

（7）如图 2-10 所示是 Active Directory 域服务安装向导的欢迎界面，单击“下一步”按钮。

（8）在弹出的“操作系统兼容性”对话框中单击“下一步”按钮。

（9）在弹出的“选择某一部署配置”对话框中选择“在新林中新建域”，因为这是林中的第一个域控制器，如图 2-11 所示。

（10）单击“下一步”按钮，在对话框“命名林根域”中输入新域的域名 dhynet.com，如图 2-12 所示。

图 2-10　Active Directory 域服务安装向导

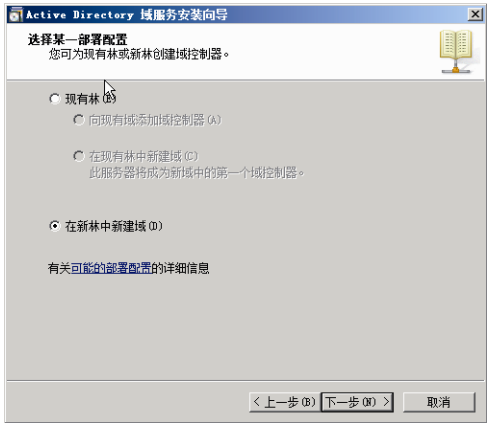

图 2-11　选择“在新林中新建域”

（11）单击“下一步”按钮，在“设置林功能级别”对话框中，选择 Windows Server 2003，如图 2-13 所示。

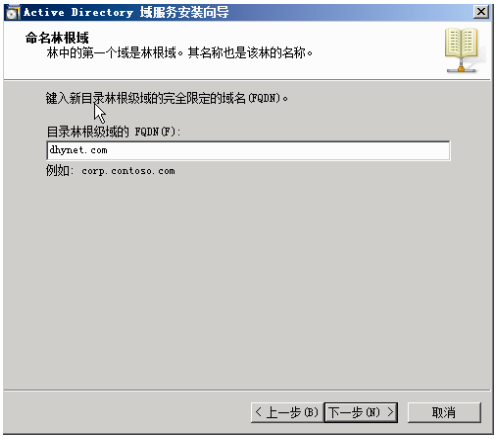

图 2-12　“命名林根域”对话框

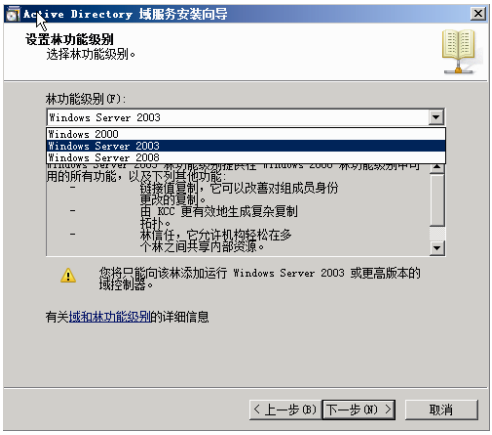

图 2-13　“设置林功能级别”对话框

说明：这里有 Windows 2000、Windows Server 2003 和 Windows Server 2008 三个选项。功能级别确定了在域或林中启用的 Active Directory 域服务（AD DS）的功能。它们还将限制哪些 Windows Server 操作系统可以在域或林中的域控制器上运行。但是，功能级别不会影响哪些操作系统可以在连接到域或林的工作站和成员服务器上运行。

创建新域或新林时，请将域和林功能级别设置为您知道的环境可以支持的最高值。这样一来，就可以尽可能充分地利用许多 AD DS 功能了。例如，如果您肯定不会将运行 Windows Server 2003（或任何较早的操作系统）的域控制器添加到域或林，请选择 Windows Server 2008 功能级别。另一方面，如果您可能会取消或添加运行 Windows Server 2003 或更早版本的域控制器，请在安装期间选择 Windows Server 2003 功能级别。如果您确定不会添加这类域控制器或这类域控制器仍在使用，则安装后可以提升功能级别。您不能降低功能级别。

安装新的林时，系统会提示您设置林功能级别，然后设置域功能级别。您不能将域功能级别设置为低于林功能级别的值。例如，如果将林功能级别设置为 Windows Server 2008，则只能将域功能级别设置为 Windows Server 2008。Windows 2000 和 Windows Server 2003 域功能

级别值在“设置功能级别”向导页中不可用。此外，默认情况下随后向该林添加的所有域都将具备 Windows Server 2008 域功能级别。

在本例中，我们选择林功能级别为 Windows Server 2003。

（12）单击“下一步”按钮，在弹出的“设置域功能级别”对话框中选择“Windows Server 2003”。

（13）单击“下一步”按钮，在弹出的“其他域功能选项”对话框中，选中“DNS 服务器”，如图 2-14 所示，单击“下一步”按钮。

（14）在弹出的“数据库、日志文件和 SYSVOL 的位置”对话框中，选择数据库文件、日志文件和 SYSVOL 的存储位置，为了获得更好的性能和可恢复性，请将数据库和日志文件存储在不同的卷上，不要把它们存储在系统盘。本例作为实验，使用默认位置，如图 2-15 所示。

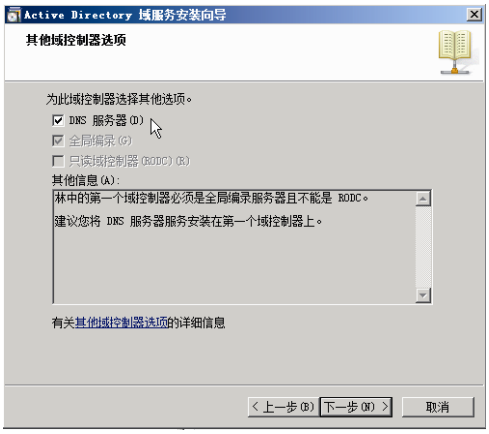

图 2-14　选中“DNS 服务器”

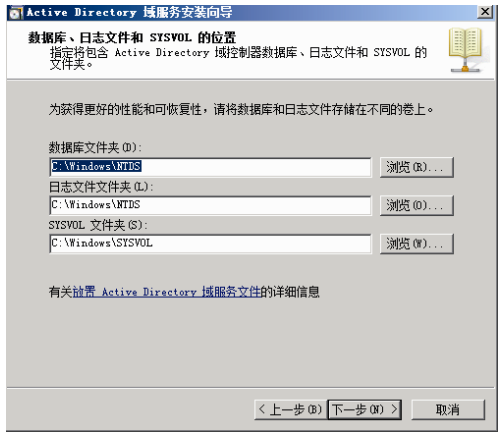

图 2-15　设置“数据库、日志文件和 SYSVOL 的位置”

（15）单击“下一步”按钮，在弹出的“目录服务还原模式的 Administrator 密码”对话框中设置还原模式的密码，如图 2-16 所示。还原模式是 Active Directory 域服务（AD DS）未运行（因为 AD DS 已停止或因为域控制器已在 DSRM 中启动）时的一种模式，这种模式下原来的域控制器的密码不再起作用，这时要登录域控制器必须有目录服务还原模式（DSRM）的密码。

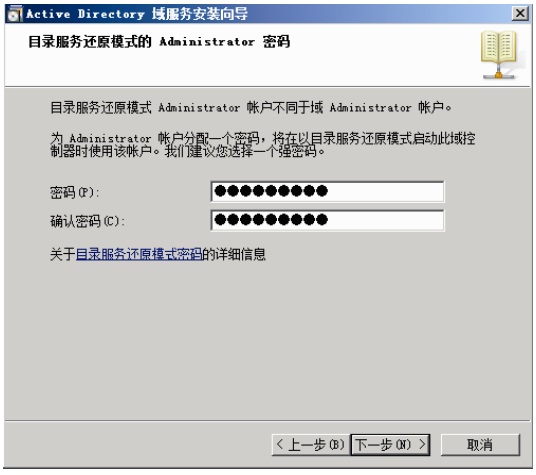

图 2-16　设置“目录服务还原模式的 Administrator 密码”

（16）单击“下一步”按钮，弹出“摘要”对话框，在“摘要”对话框中单击“下一步”按钮，开始安装 AD DS 服务。安装完成后，重启计算机，安装完成。

2.3.2　任务 2：确认域控制器是否安装正常及故障排除

1．通过创建用户和用户登录验证

可以通过在 AD 中添加用户账户，然后使用此账户在另外一台计算机登录域的方法确认域控制器是否安装正常。

在 AD 中添加账户 student-1，登录名为 s1，然后以 s1 的登录名从另外一个 Windows 7 计算机上登录到域。

注意：账户名与登录名可以不一样，在不一样时请区分账户名与登录名。

（1）在域控制器上，单击“开始”→“管理工具”→“Active Directory 用户和计算机”，在打开的窗口中展开“dhynet.com”，右击“Users”，选择“新建”→“用户”命令，如图 2-17 所示。

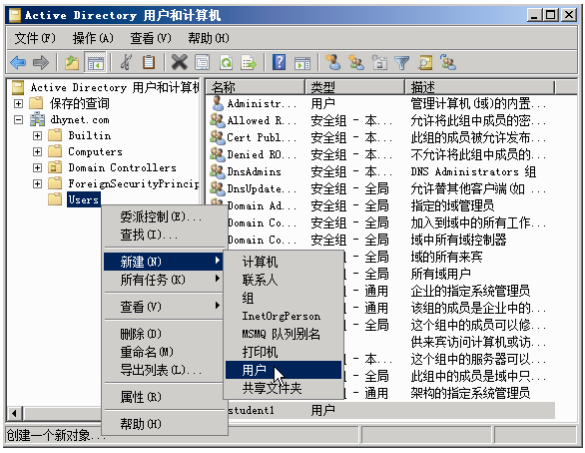

图 2-17　新建用户

（2）在“新建对象-用户”对话框中，输入用户信息，如图 2-18 所示。单击“下一步”按钮。

注意：账户名与登录名可以不一样。

（3）输入用户密码，取消勾选“用户下次登录时须更改密码”复选框，如图 2-19 所示。单击“下一步”按钮，完成用户创建。

图 2-18　输入用户信息

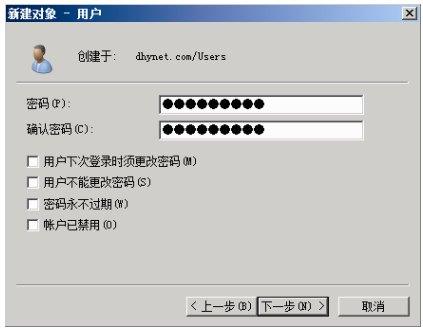

图 2-19　设置用户密码

注意：取消勾选“用户下次登录时须更改密码”选项是为了做实验时简单一些，避免用户下次登录要更改密码的麻烦。在真实环境中，用户首次登录后应该让用户自己设置自己的密码，也就是要勾选此项。

下面把另外一台安装 Windows 7 的计算机加入域，并使用刚才新建的用户 student-1 登录。

（4）开启另外一台安装 Windows 7 的计算机，这台计算机名为 WIN-7。设置该计算机的 IP 地址与 dhynet.com 域控制器在同一个段，首选 DNS 地址为域 dhynet.com 的 DNS 地址。

（5）单击“开始”按钮，右击“计算机”→“属性”，在打开的“系统”对话框中选择“计算机名称、域和工作组设置”选项组中的“更改设置”命令链接，如图 2-20 所示。

图 2-20　“系统”对话框

（6）在弹出的“系统属性”对话框中的“计算机名”选项卡中单击“更改”按钮，如图 2-21 所示。

（7）在“计算机名/域更改”对话框中选择“隶属于”选项组中的“域”，在域名中填写“dhynet.com”，如图 2-22 所示。单击“确定”按钮。

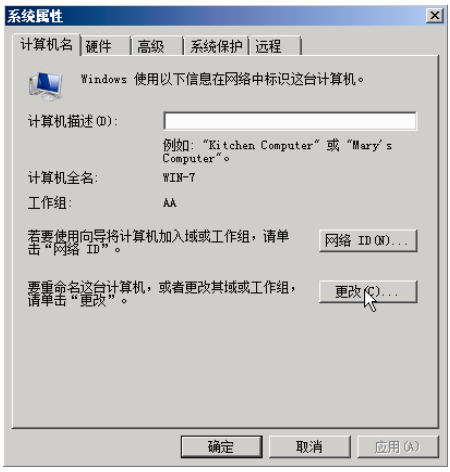

图 2-21　更改计算机名

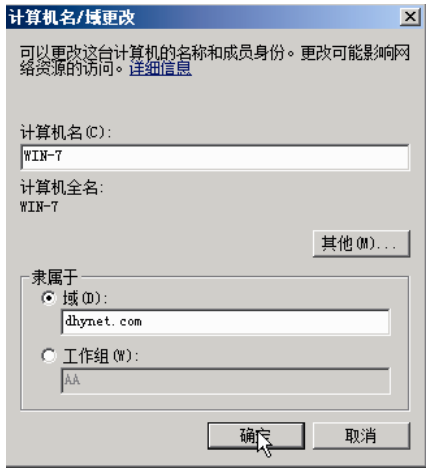

图 2-22　“计算机名/域更改”对话框

（8）在弹出的“Windows 安全”对话框中填写用户名 s1，以及用户的密码，如图 2-23 所示。单击两次“确定”按钮，重启计算机。

（9）重启后单击“切换用户”，输入用户名 s1，输入密码，选择登录到 DHYNET。如图 2-24 所示。

图 2-23　输入域用户名和密码

图 2-24　登录到域

注意：s1 这个用户并不是在 WIN-7 这台计算机中创建的，而是在域控制器中创建的，但是却能够从 WIN-7 这台计算机中登录。事实上用户 s1 默认不能从域控制器中登录，但能从域中的其他计算机上登录。

如果登录成功，说明 AD 创建正常，如果不能登录，请参照下面的内容检查 DNS 服务器内的记录是否完备。

2．检查 DNS 服务器内的记录是否完备

由于域控制器会将自己登记到 DNS 服务器内，以便让其他的计算机通过 DNS 服务器查找这个域控制器。因此，应首先检查 DNS 服务器内是否已经有这些域控制器的数据。

首先要检查的是域控制器是否已将其主机名称与 IP 地址登记到了 DNS 服务器内。请到扮演 DNS 服务器角色的计算机上选择“开始”→“管理工具”→“DNS”，如图 2-25 所示会有一个名称为 dhynet.com 的区域，它让 Windows Server 2008 域 dhynet.com 中的成员（域控制器、成员服务器、Windows 7、Windows XP Professional 等）将其数据登记到这个区域中。在图 2-25 中右侧的记录，表示域控制器 win-662ohffgg1z.dhynet.com 已经正确地将其主机名称与 IP 地址登记到 DNS 服务器内。

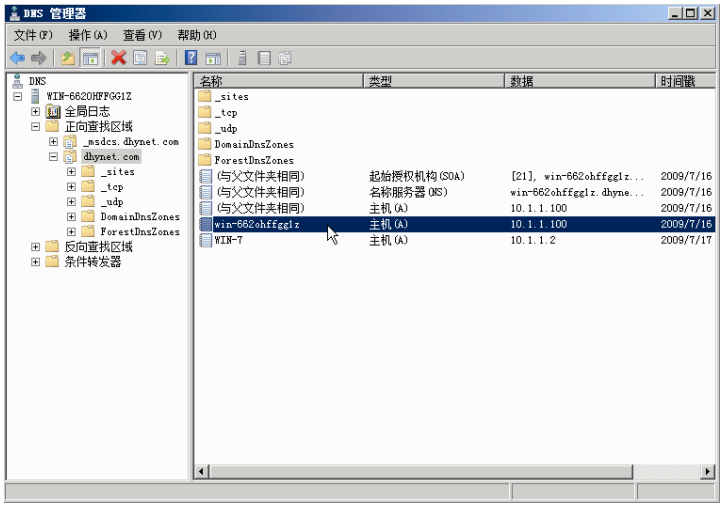

图 2-25　查看 DNS

如果域控制器已经将其与活动目录有关的数据登记到了 DNS 服务器内，则应该会有如图 2-25 左侧所示的文件夹，如_tcp、_udp 等。在单击_tcp 文件夹后，将看到如图 2-26 所示的

画面，其中数据类型为 SRV 的_ldap 记录表示 win-662ohffgg1z.dhynet.com 已经正确地将其扮演域控制器角色的事项登记到了 DNS 服务器。从图中的_gc 还可以看出“全局编录”的角色是由 win-662ohffgg1z.dhynet.com 所扮演的。

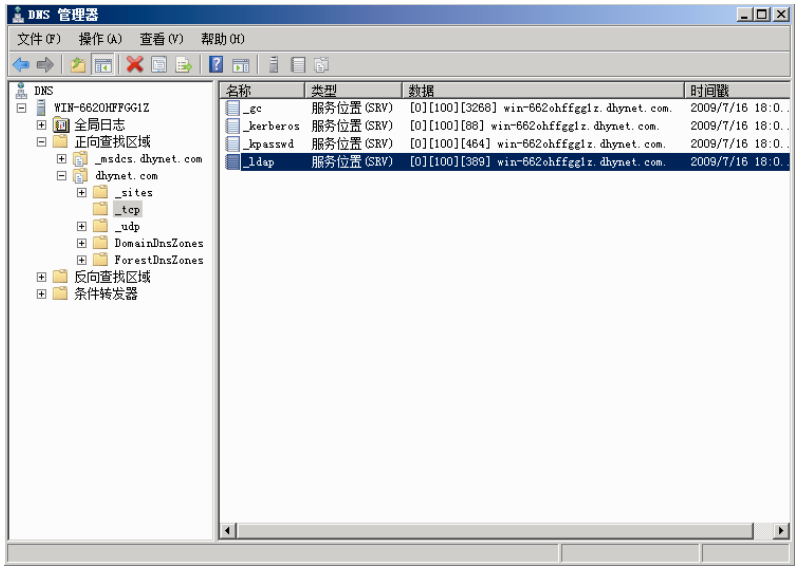

图 2-26　查看 SRV 数据类型的记录

如果没有出现上述_tcp 等文件夹与相关数据，则请到该域控制器上利用“开始”→“管理工具”→“服务”→右击“Net Logon”服务→“重新启动”的方式登记。

2.3.3　任务 3：额外域控制器的创建

创建额外域控制器的目的有两个。

- 提供容错功能，因为即使一个域控制器发生故障了，仍然能够有另一个额外的域控制器提供服务。
- 可以改善用户登录的效率。多个域控制器可以分担审核用户身份的负担。

（1）假设额外域控制器安装在计算机 win2k8-1 上，设置 win2k8-1 的首选 DNS 服务器为安装独立域控制器的计算机所使用的 DNS 服务器。比如，前面安装独立域控制器时集成了 DNS 服务器（域控制器与 DNS 服务器在同一台计算机上），因此设置 win2k8-1 的首选 DNS 为域控制器的 IP 地址 10.1.1.100。

（2）单击“开始”→“运行”命令，然后输入 dcpromo 以打开“Active Directory 域服务安装向导”，单击“下一步”按钮。

（3）在“操作系统兼容性”页中阅读有关信息，然后单击“下一步”按钮。

（4）在“选择某一部署配置”页面上，单击“现有林”→“向现有域添加域控制器”，如图 2-27 所示。然后单击“下一步”按钮。

（5）在“网络凭据”页中，输入林的名字 dhynet.com，单击“设置”，输入要用于该操作的用户账户的用户名、密码及用户域，如图 2-28 所示。然后单击“确定”和“下一步”按钮。

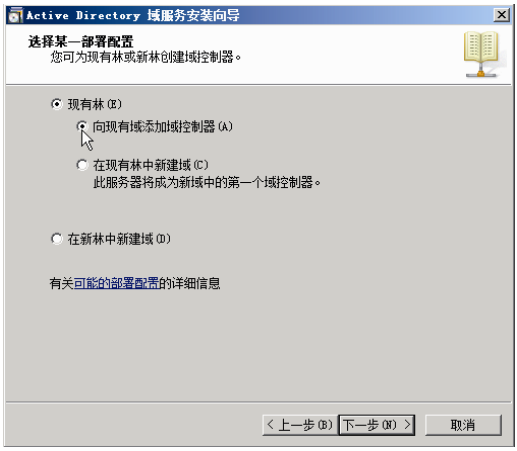

图 2-27　向现有域添加域控制器

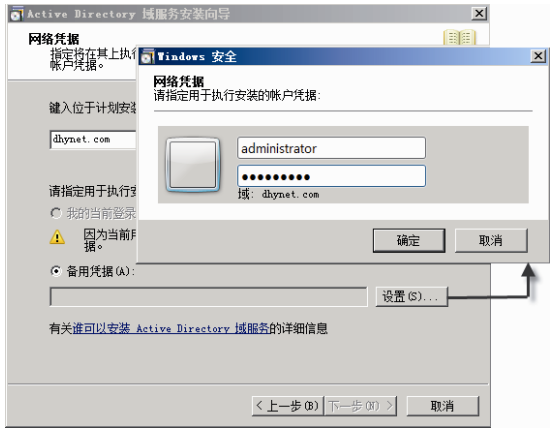

图 2-28　输入域管理员的用户名和密码

此用户账户必须是目标域 dhynet.com 的 Domain Admins 组的成员，如 administrator。

（6）在“选择一个域”页中，选择要创建额外域控制器的域。选择 dhynet.com，如图 2-29 所示。然后单击两次“下一步”按钮，

（7）在“其他域控制器选项”页中选中“DNS 服务器”和“全局编录”，如图 2-30 所示，单击“下一步”按钮。

图 2-29　选择要创建额外域控制器的域

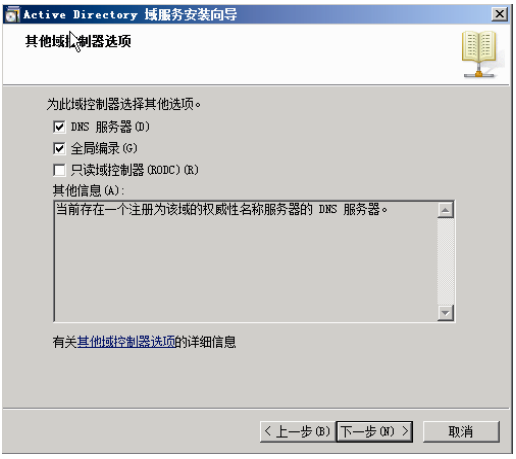

图 2-30　“其他域控制器选项”页

（8）进入指定“数据库、日志文件和 SYSVOL 的位置”页面，输入要安装数据库、日志文件和 SYSVOL 的位置，或单击“浏览”按钮，选择一个位置，然后单击“下一步”按钮，

（9）在弹出的“目录服务还原模式的 Administrator 密码”对话框中设置还原模式的密码后，单击“下一步”按钮。

（10）检查“摘要”页面，然后单击“下一步”按钮开始安装。

注意：此时的安装过程与独立域控制器的安装不一样，额外域控制器的安装是从独立域控制器中复制数据。安装过程的动画形象地展示了它的复制特性，如图 2-31 所示。

（11）重新启动计算机完成安装。

图 2-31　额外域控制器的安装界面

2.3.4　任务 4：子域的创建

现在通过创建 dhynet.com 的子域 bg.dhynet.com，来说明子域的创建方法。

安装子域与安装独立域控制器和额外域控制器的步骤大致相同，可以参考对照前面安装独立域控制器和额外域控制器的步骤说明。

（1）假设子域控制器安装在计算机 win2k8-2 上，设置 win2k8-2 的首选 DNS 服务器为安装独立域控制器所使用的 DNS 服务器。比如，前面在计算机 win2k8 上安装独立域控制器使用的 DNS 是在 win2k8 本机上安装的 DNS 服务器，因此设置 win2k8-2 的首选 DNS 为 win2k8 的 IP 地址 10.1.1.100。

（2）单击“开始”→“运行”命令，然后输入 dcpromo，启动“Active Directory 安装向导”。

（3）在“操作系统兼容性”页中阅读有关信息，然后单击“下一步”按钮。

（4）如果这是您首次在运行 Windows Server 2008 的服务器上安装 Active Directory，请单击“兼容性帮助”以获得更多信息。

（5）单击“选择某一部署配置”页面上的“现有林”→“在现有林中新建域”，如图 2-32 所示。然后单击“下一步”按钮。

（6）在“网络凭据”对话框中，输入林的名字 dhynet.com，单击“设置”按钮，输入要用于该操作的用户账户的用户名、密码及用户域，如图 2-33 所示。然后单击“确定”和“下一步”按钮。

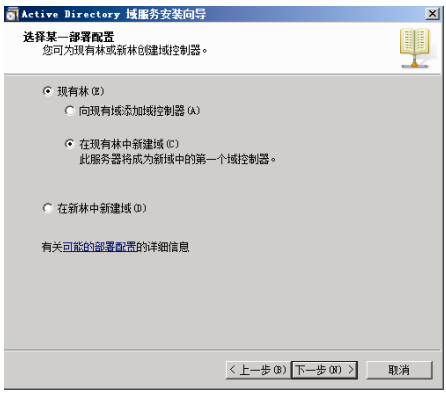

图 2-32　新建子域

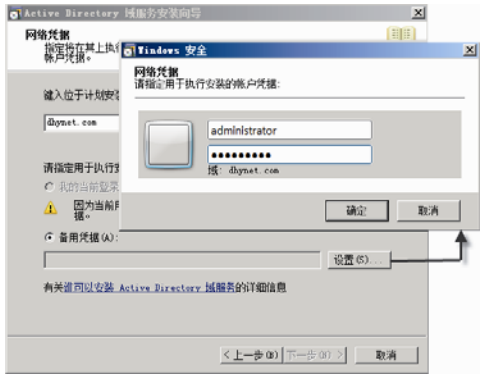

图 2-33　输入网络凭据

此用户账户必须是目标域 dhynet.com 的 Domain Admins 组的成员，如 administrator。

（7）在“命名新域”页中确认父域的名称，输入子域的 DNS 名称，如图 2-34 所示。单击“下一步”按钮。

（8）在“域 NetBIOS 名称”页上，验证 NetBIOS 名称，然后单击“下一步”按钮。

（9）在图 2-35 中，设置域功能级别。域功能级别的设置参见本章的相关内容。单击 3 次“下一步”按钮。

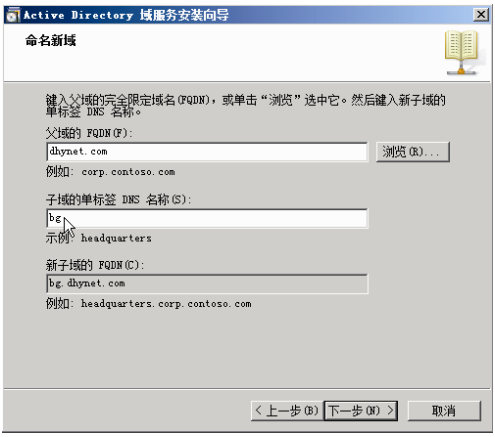

图 2-34　“命名新域”页

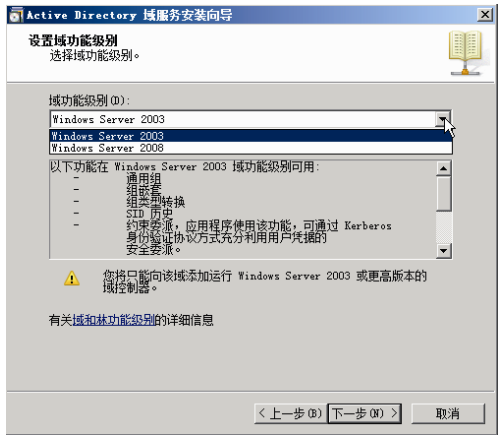

图 2-35　“设置域功能级别”页

（10）在“数据库和日志文件文件夹”页面上，输入要安装数据库和日志文件文件夹的位置，或单击“浏览”选择一个位置，然后单击“下一步”按钮。

（11）在“共享的系统卷”页面上，输入要安装 Sysvol 文件夹的位置，或单击“浏览”选择一个位置，然后单击“下一步”按钮。

（14）在“目录服务还原模式的管理员密码”页面上，输入在“目录服务还原模式”下启动此计算机时使用的密码。然后单击“下一步”按钮。

（15）检查“摘要”页面，然后单击“下一步”按钮开始安装。

（16）重新启动计算机完成安装。

注意：

- 要执行此过程，您必须是 Active Directory 中 Domain Admins 组（在父域中）或 Enterprise Admins 组的成员，或者您必须已被授予适当的权限。作为安全性的最佳操作，请考虑使用运行方式来执行这个过程。
- 使用该过程安装 Active Directory 的服务器将是新子域中的第一个域控制器。
- 当子域被添加到现有的树域中时，默认情况下将建立一个双向、可传递的父子信任。

2.3.5　任务 5：删除活动目录

如果你想删除域，或者把域控制器降级为成员服务器或者独立服务器，就需要删除活动目录。

（1）在域控制器服务器计算机上单击“开始”→“运行”，输入 dcpromo 命令，按回车键。

（2）在“Active Directory 域服务安装向导”中单击“下一步”按钮。

（3）如果出现如图 2-36 所示的对话框，表示这台域控制器是一台“全局编录”服务器，在将其降级为一般的 Windows Server 2008 后，它将不再扮演“全局编录”的角色。因此，请

先确定网络上是否还有其他的“全局编录”服务器。

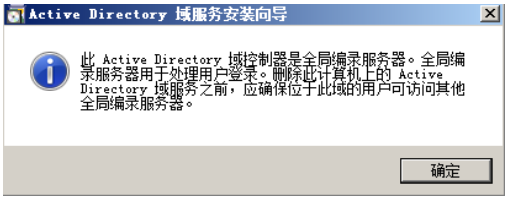

图 2-36　确认是否全局编录

（4）如果这台计算机是域内的最后一个域控制器，请选中“删除该域，因为此服务器是该域中的最后一个域控制器”，则降级后这台计算机将变成独立服务器，否则将变成这个域的成员服务器，如图 2-37 所示。

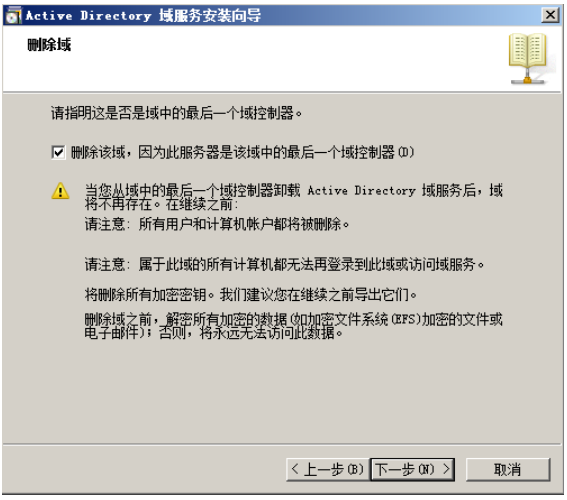

图 2-37　确认是否是最后一个域控制器

（5）两次单击“下一步”按钮，出现如图 2-38 所示的对话框，按图中所示进行设置，单击“下一步”按钮。

（6）在图 2-39 中选中选项以删除 DNS 委派。单击“下一步”按钮，输入有权限删除 DNS 区域的管理员密码（即管理凭据）。

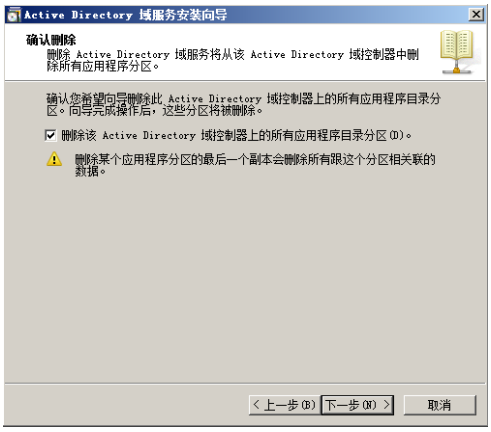

图 2-38　删除应用程序目录分区

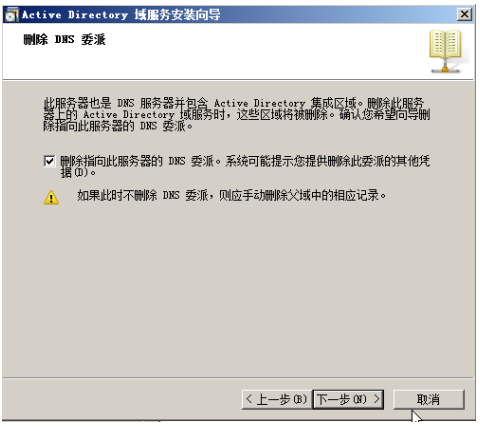

图 2-39　删除 DNS 委派

（7）输入新的管理员密码。这个新管理员是指删除 AD 后，域控制器降级为成员服务器或者独立服务器的本地管理员密码，如图 2-40 所示。

图 2-40　设置新的管理员密码

（8）单击两次“下一步”按钮，完成后重启计算机，AD 被删除，域控制器降级为成员服务器或者独立服务器。

2.4　知识能力拓展案例 2：创建森林

2.4.1　工作情景描述

DHYNET 公司兼并了 ABC 公司，为了公司的统一管理，决定为 ABC 公司建立 abc.net 域，并且把 abc.net 域加入到现有的 dhynet.com 域林中。

2.4.2　案例分析

当在单位中创建第一个域控制器时，也就是在创建第一个域（也称为“林根”域）和第一个林。比如，创建了 dhynet.com 域时也就创建了一个域林。

最上层 Active Directory 容器被称为林。林由一个或多个共享公共架构和全局编录的域组成。一个单位可以有多个林。

林是驻留在该林内的所有对象的安全和管理边界。相对而言，域是管理对象（如用户、组和计算机）的管理边界。此外，每个域都有单独的安全策略和与其他域的信任关系。

单个林内的多个域树不能构成连续的名称空间，它们有着不连续的 DNS 域名，如 dhynet.com 与 abc.net。尽管林中的树不共享名称空间，但一个林确实只有一个根域，称为林根域。根据定义，林根域是林中创建的第一个域，在这个案例中就是 dhynet.com。Enterprise Admins 和 Schema Admins 组就位于此域中。默认情况下，这两个组的成员有林范围的管理权限。

2.5　案例 2 实施过程

（1）单击“开始”→“运行”命令，然后输入 dcpromo，启动“Active Directory 安装向

导”，勾选“使用高级模式安装”，如图 2-41 所示。单击“下一步”按钮。

（2）在“操作系统兼容性”页中阅读有关信息，然后单击“下一步”按钮。如果这是您首次在运行 Windows Server 2008 的服务器上安装 Active Directory，请单击“兼容性帮助”以获得更多信息。

（3）在“选择某一部署配置”页面上选择“现有林”→“在现有林中新建域”→“新建域树根而不是新子域”，然后单击“下一步”按钮，如图 2-42 所示。

图 2-41　必须使用高级模式安装

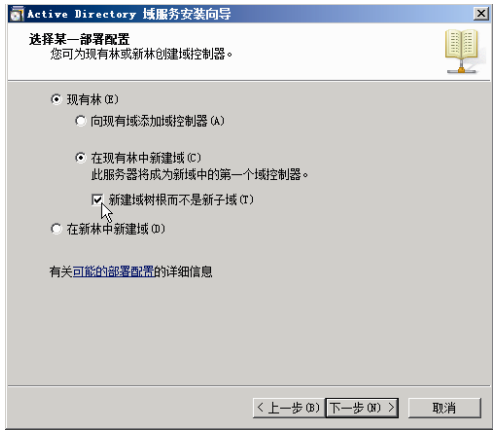

图 2-42　选择创建森林

（4）在“网络凭据”页中，输入林的名字 dhynet.com，单击“设置”按钮，输入要用于该操作的用户账户的用户名、密码及用户域，此用户账户必须是 Enterprise Admins 组的成员，如图 2-43 所示。然后单击“确定”和“下一步”按钮。

（5）在“命名新域树根”页面上，输入新域的 DNS 全名 abc.net，然后单击“下一步”按钮，如图 2-44 所示。

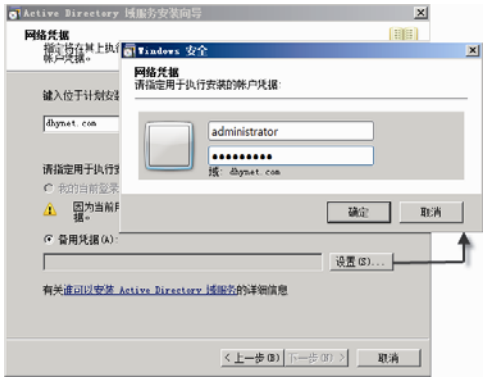

图 2-43　输入网络凭据

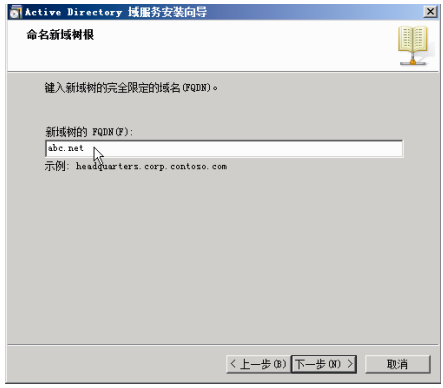

图 2-44　命名新域树

（6）验证“NetBIOS 域名”页面上的 NetBIOS 名称，然后单击“下一步”按钮。

（7）设置域功能级别，单击 2 次“下一步”按钮。

（8）在图 2-45 中，选中“全局编录”，单击“下一步”按钮。

说明：本例中，本计算机已经安装了 DNS 服务，所以 DNS 处于不能选中状态。如果计算

机中没有安装 DNS 服务，要选中“DNS 服务器”。

（9）在图 2-46 中，确认选中“让向导选择一个合适的域控制器”，单击“下一步”按钮。

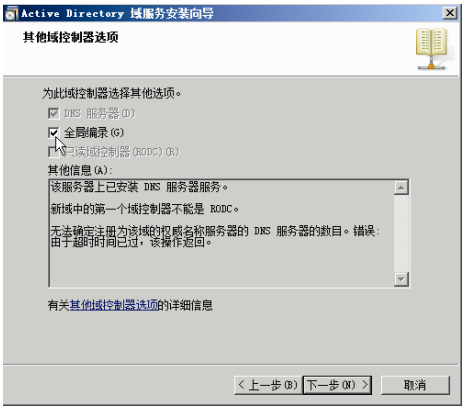

图 2-45　选中全局编录

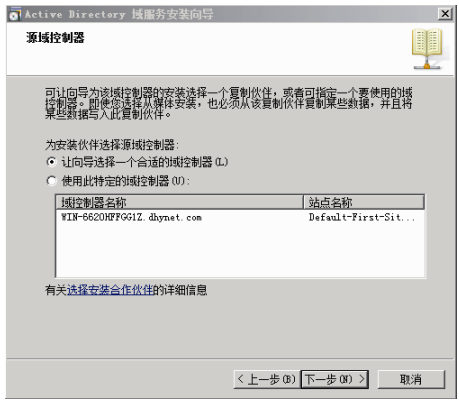

图 2-46　让向导选择一个合适的域控制器

（10）在“数据库和日志文件文件夹”页面上，输入要安装数据库和日志文件文件夹的位置，或单击“浏览”选择一个位置，然后单击“下一步”按钮。

（11）在“共享的系统卷”页面上，输入要安装 Sysvol 文件夹的位置，或单击“浏览”选择一个位置，然后单击“下一步”按钮。

（12）在“目录服务还原模式管理员密码”页面上，输入并确认要指派给该服务器管理员账户的密码，然后单击“下一步”按钮。

（13）检查“摘要”页面，然后单击“下一步”按钮开始安装。

（14）重新启动计算机完成安装。

2.6　项目完成结论

Microsoft Active Directory 服务是 Windows 平台的核心组件，Active Directory 存储了有关网络对象的信息，这些对象包括用户、用户组、计算机、域、组织单位（OU）、组、文件、打印机、应用程序、服务器及安全策略等。Active Directory 为管理员对这些对象进行组织和管理提供了一种有力的手段。

通过创建额外的域控制器，以提供容错功能。这样即使一个域控制器发生故障了，仍然能够有另一个额外的域控制器提供服务。可以改善用户登录的效率。多个域控制器可以分担审核用户身份的负担。

通过创建子域，可以分层管理域，还可以实施委托管理。

2.7　练习案例

天唐公司有下属部门销售部、市场部、财务部等。公司现有 5 台服务器，500 台客户机。计划使用域结构网络管理公司的网络和用户，要求域控制器具有容错功能。请你为公司设计域树结构并实施。

2.8　课后习题

1．WTO 公司准备使用一台服务器作为公司域中附加的域控制器，那么该服务器上可以选择安装的 Windows Server 2008 版本有（　　）。（选择 3 项）

A．Windows Server 2008 桌面版　　B．Windows Server Web 版

C．Windows Server 2008 数据中心版　　D．Windows Server 2008 企业版

E．Windows Server 2008 标准版

2．某网络管理员在将一台位于工作组中的计算机加入域中时出现如下所示的错误提示，可能会导致这种情况的原因有（　　）。

A．DNS 中没有配置这台计算机的域名

B．没有为域配置相应的 NetBIOS 名称

C．没有为这台计算机配置正确的 DNS 服务器地址

D．域控制器和这台计算机不在同一个 IP 子网中

3．你想将一台工作组中的 Windows Server 2008 服务器升级成域控制器，可以使用下列方法（　　）。（选择 2 项）

A．管理您的服务器　　B．Windows 组件向导

C．设备管理器　　D．dcpromo 命令

4．公司需要使用域控制器来集中管理域账户，你安装域控制器必须具备以下条件（　　）。（选择 2 项）

A．操作系统版本是 Windows Server 2003 或者 Windows XP

B．本地磁盘至少有一个 NTFS 分区

C．本地磁盘必须全部是 NTFS 分区

D．有相应的 DNS 服务器支持

项目 3　DHCP 服务的安装、配置与管理

在规模企业中是否需要网络管理员手动配置 IP 地址呢？答案是否定的。因为 Windows Server 2008 网络中 DHCP 服务器可以提供该服务。本章的主要目的是要说明在 Windows Server 2008 网络中如何利用动态主机配置协议（DHCP），深入理解 DHCP 及其运作原理将有助于系统管理员有效地分配网络中的 IP 地址。同时，本章初步介绍了什么是动态地址，动态地址在企业应用中的好处和场景，如何在企业中管理和配置 DHCP 服务器。学习完本章后，应能够掌握以下知识技能点，并在实际操练中能够掌握 DHCP 服务器的相关配置和日常管理。

知识点、技能点

- 了解 DHCP 在网络中的作用
- 掌握 DHCP 服务器的安装方法
- 能够配置 DHCP 作用域
- 能够配置 DHCP 选项
- 能够配置 DHCP 保留

3.1　引例：为什么使用 DHCP 服务器（WHY）

在一个企业中，有 500 台计算机。为了能够正常使用网络，每个计算机需要设置一个 IP 地址，管理员手动到每台机器上设置 IP 地址显然是一个浩大的工程。即便是手动设置完了，一旦网络中的计算机有变化，则需要再次进行设定，这对于网络管理员来说，犹如是一场恶梦。如何来简化这个过程，让管理员从繁重的 IP 设置中解脱出来，去做更重要的网络维护任务呢？

我们可以采用 DHCP 服务器来解决这个问题。DHCP 是 Dynamic Host Configuration Protocol（动态主机分配协议）的缩写，它可以简化网络中的 IP 地址分配工作。一般来说，设定 IP 地址的方法有两种。

（1）手动设置 IP 地址。这种方法需要在每个客户端手动设置 IP 地址及相关选项，工作量大，费时费力，且容易导致 IP 问题出现，进而影响客户机网络使用，如 IP 地址冲突等。一旦发生这样的问题，追踪源头会很困难。另外，如果把客户机从一个网络，搬到另一个网络中，则需要再次进行设定。

（2）自动设置 IP 地址。利用 DHCP 服务器，来进行客户端 IP 地址的自动分配。这意味着管理员不需要到每台客户机上去手动设置 IP 地址，而是由 DHCP 服务器来完成这个工作，并且不会出现 IP 地址冲突的情况。

手动 IP 设置与自动 IP 设置的对比如表 3-1 所示。

表 3-1　手动 IP 设置与自动 IP 设置对比

手动 IP 设置	自动 IP 设置
必须在每台客户端上输入 IP 地址	DHCP 服务器自动为客户端计算机提供 IP 地址
可能输入错误或无效的 IP 地址	确保网络中的客户端使用正确的配置信息
错误的配置可能导致通信问题和网络问题	排除一系列由 IP 地址而导致的常见网络问题的来源
对于计算机在子网间频繁移动的网络来说，增加了管理上的开销	客户端配置自动更新以反映网络结构的变化

使用 DHCP 自动分配 IP 地址，当客户端连入网络，并发出 IP 地址请求时，DHCP 服务器从 IP 地址池中临时分配一个 IP 地址给客户端，当客户端不使用时，DHCP 服务器可以收回这个 IP，并把它分配给其他有需要的客户端。这样可以有效节约 IP 地址，既保证了客户机的网络通信，又提高了 IP 地址的使用率，如图 3-1 所示。

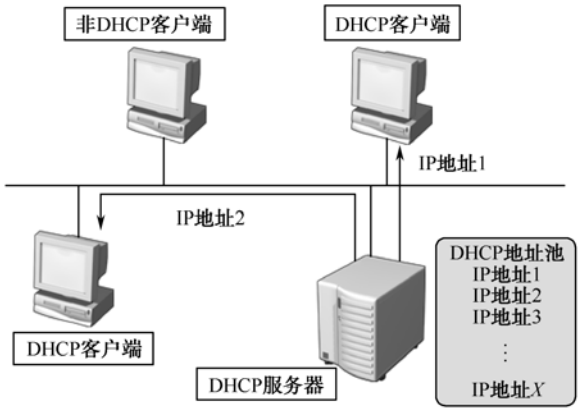

图 3-1　DHCP 分配 IP

3.2　案例：IP 地址自动管理

3.2.1　工作情景描述

你是公司的网络管理员，公司有一个单域环境，域名是 dhynet.com，网络地址为 192.168.2.0/24。域中有 200 台计算机，为了方便用户使用网络，所有的计算机都需要能自动获取 IP 地址，并且能够自动获取网关及 DNS 配置信息。另外，Web 服务器与 FTP 服务器要求 IP 地址能够固定，分别使用 192.168.2.66 和 192.168.2.88 作为自己计算机的 IP 地址。作为管理员，你要如何解决这些问题？

3.2.2　案例分析

（1）在本项目中，为了让客户端能够自动获取 IP 地址，在网络中必须安装 DHCP 服务器。

（2）DHCP 服务器需要配置相应的作用域，生成 IP 地址池，以供客户机申请使用。

（3）DHCP 服务器在给客户端提供 IP 地址的同时，还需要为客户端提供网关地址和 DNS 地址等信息，让客户端在获得 IP 地址的同时，也能够获取这些信息，并配置使用。

（4）DHCP 服务器还需要针对 Web 服务器和 FTP 服务器对 IP 地址的特殊需求，进行设置，使它们能够获得固定的 IP 地址。

注：非 DHCP 客户端指的是不支持自动获取 IP 地址的客户端。现在的主流操作系统均支持自动获取功能。

3.2.3　相关知识

DHCP 服务器的工作原理，如图 3-2 所示。

DHCP 客户端自动获取 IP 地址的过程，由 4 个步骤完成。

（1）客户端发送 DHCP DISCOVER（广播形式）。当 DHCP 客户端第一次登录网络的时候，也就是客户发现本机上没有任何 IP 数据设定的时候，它会向网络发出一个 DHCP DISCOVER 封包，向网络中寻求 DHCP 服务。

（2）DHCP 服务器回应 DHCP OFFER（广播形式）。DHCP 服务器会从那些还没有租出的地址范围内，选择最前面的空置 IP ，连同其他 TCP/IP 设定，响应给客户端一个 DHCP OFFER 封包。

（3）客户端回应 DHCP REQUEST（广播形式）。如果客户端收到网络上多台 DHCP 服务器的响应，只会挑选其中一个 DHCP OFFER（通常是最先抵达的那个），并且会向网络发送一个 DHCP REQUEST 广播封包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。

（4）DHCP 服务器响应 DHCP ACK（广播形式）。当 DHCP 服务器接收到客户端的 DHCP REQUEST 之后，会向客户端发出一个 DHCP ACK 响应，以确认 IP 租约的正式生效，也就结束了一个完整的 DHCP 工作过程。

租约的更新。客户端在获取到 IP 地址信息时，同时会产生租约时间（默认为 8 天）。当使用 IP 地址时间达到租约时间的 50%时，客户端开始进行续约操作，续约成功则继续使用当前 IP 地址，并更新租约时间。如果此时续约不成功，则在租约时间达到 87.5%时再次续约，如果仍不能续约，客户端则开始进行重新开始租约过程，即重新获取 IP 地址。

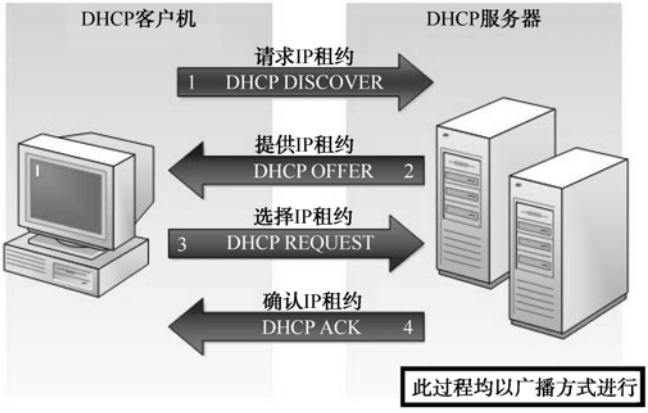

图 3-2　DHCP 服务器工作原理

3.3　案例实施过程

3.3.1　任务 1：DHCP 服务器角色的安装

1．案例分析

为了能够提供 DHCP 服务，让客户机能自动获得 IP 地址，作为管理员来说，需要在网络中安装 DHCP 服务器。在 Windows Server 2008 系统中默认没有安装 DHCP 服务器，因此需要安装 DHCP 服务器。安装 DHCP 的机器要使用固定 IP（本例中使用 192.168.2.254），在安装

DHCP 服务器功能前必须设定完成。

2．实施过程

（1）单击“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口，单击“角色”，如图 3-3 所示。

图 3-3　添加服务器角色

（2）单击“添加角色”，然后单击“服务器角色”，即可对所要添加的角色进行选择，如图 3-4 所示，单击“下一步”按钮。

注意：如果此时服务器还未配置固定 IP 地址，则系统会进行提示，为保证 DHCP 服务器工作正常，请在安装 DHCP 服务器前设置好固定 IP 地址。

图 3-4　勾选“DHCP 服务器”角色

（3）此时会出现 DHCP 服务器简介及注意事项，阅读了解之后，单击“下一步”按钮。出现如图 3-5 所示的窗口，显示出本机所绑定的 IP 地址，选择要设定为服务器所使用的 IP 地址，单击“下一步”按钮。

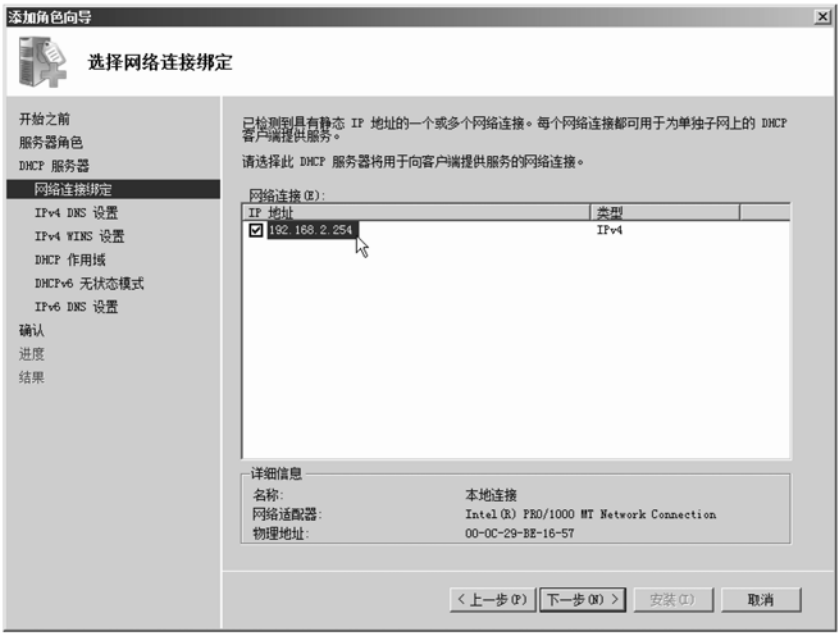

图 3-5　设定服务器的 IP 地址

（4）在出现的父域及 DNS 设定窗口中，设置父域名称信息和 DNS 服务器地址信息，如图 3-6 所示。如果不指定，则直接单击“下一步”按钮。

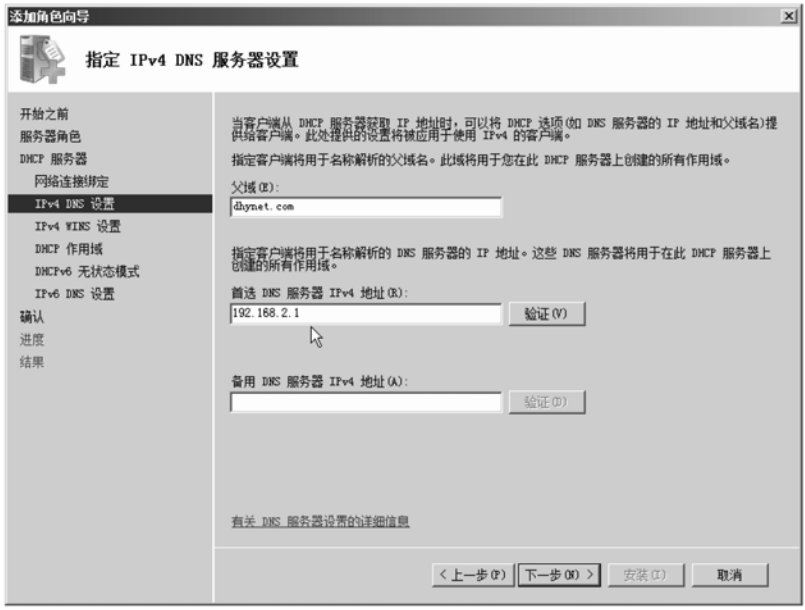

图 3-6　设置 DNS 服务器信息

（5）此时，出现的是 WINS 服务器地址信息设定窗口，如图 3-7 所示。此处我们不设置，直接单击“下一步”按钮。

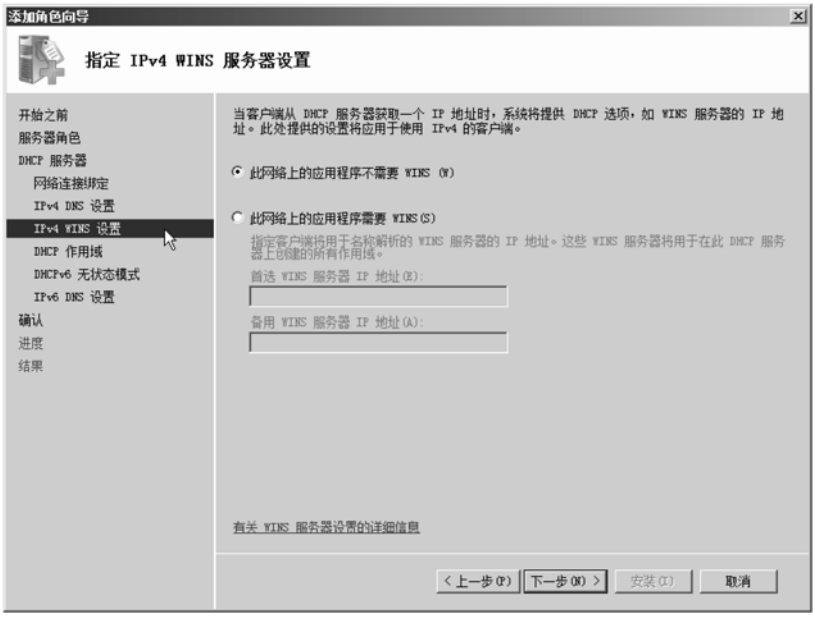

图 3-7　设置 WINS 服务器信息

（6）系统弹出“添加作用域”窗口，如图 3-8 所示。根据实际情况，填入相关信息，并勾选“激活此作用域”，然后单击“下一步”按钮。

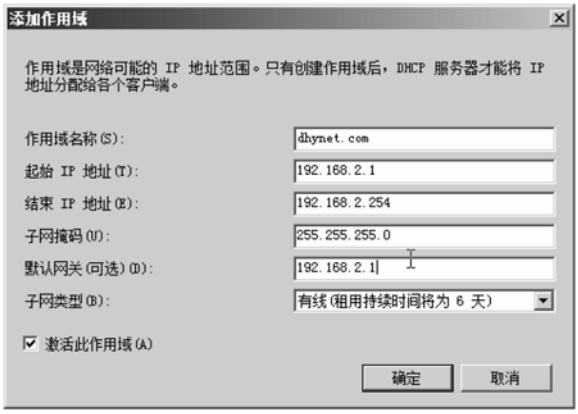

图 3-8　设置作用域信息

（7）此时，将出现 IPV6 的相关设置窗口，可以根据实际情况进行设定。本例中，我们不涉及 IPV6，因此直接单击两次“下一步”按钮，跳过对 IPV6 的设定。

（8）系统弹出“确认安装选择”窗口，在窗口中列出了对 DHCP 服务器设定的相关总结信息，如图 3-9 所示。检查确认无误后，单击“安装”按钮。

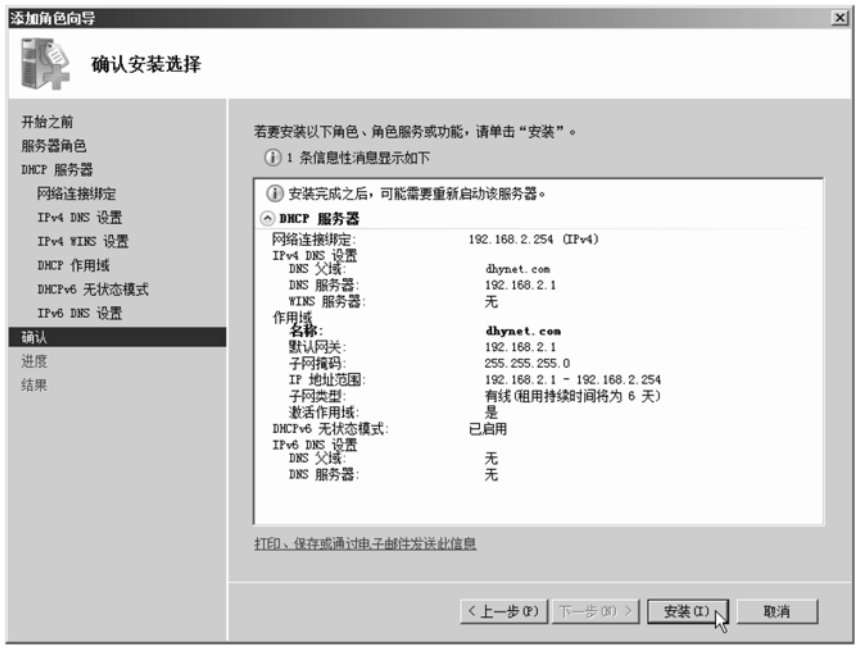

图 3-9　DHCP 服务器信息设置预览

（9）安装成功后，将会出现如图 3-10 所示的界面，表示安装成功。

图 3-10　DHCP 服务器安装成功提示

3．简要总结

在这个任务中，我们安装了 DHCP 服务器，并在安装向导的帮助下，完成了如下设置。

- 设置了 DHCP 服务器的固定 IP 地址。
- 安装 DHCP 服务器。
- 设定了父域及首选 DNS。
- 设置了起始 IP 地址和结束 IP 地址（即 IP 地址池），子网掩码和默认网关。

至此，这个 DHCP 服务器就可以满足基本应用了。在这个配置方法的配置下，DHCP 客户端可以从 DHCP 服务器上自动获取 IP 地址、子网掩码、默认网关和 DNS 的相关信息。

3.3.2　任务 2：DHCP 服务客户端的配置

1．案例分析

安装了 DHCP 服务并创建了 IP 作用域后，要想使用 DHCP 方式为客户端计算机分配 IP 地址，除了网络中有一台 DHCP 服务器外，还要求客户端计算机应该具备自动向 DHCP 服务器获取 IP 地址的能力，这些客户端计算机就被称为 DHCP 客户端。因此，你需要对客户端的 TCP/IP 属性进行一下设置。

2．实施过程

以 Win XP 为例，在桌面上右击“网上邻居”图标，执行“属性”命令。在打开的“网络连接”窗口中右击“本地连接”并单击“属性”，打开“本地连接属性”对话框。然后双击“Internet 协议（TCP/IP）”选项，点选“自动获得 IP 地址”单选框，并依次单击“确定”按钮，如图 3-11 所示。

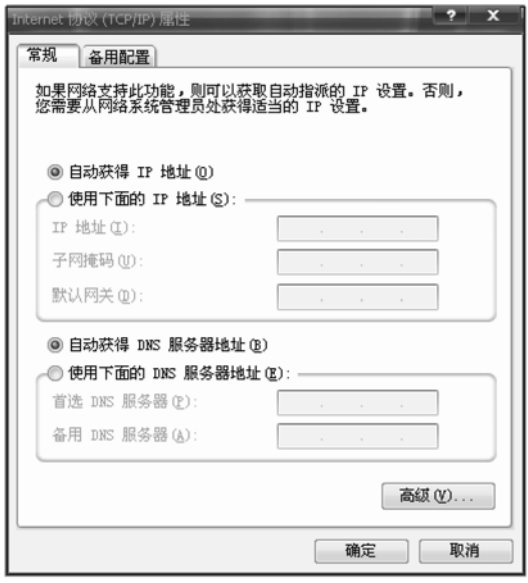

图 3-11　客户端 TCP/IP 设置

提示：默认情况下客户端计算机使用的都是自动获取 IP 地址的方式，一般无须进行修改，只需检查一下即可。

至此，DHCP 服务器端和客户端已经全部设置完成了。在 DHCP 服务器正常运行的情况下，首次开机的客户端会自动获取一个 IP 地址并拥有 8 天的使用期限。

客户端查看获取 IP 情况的方法：单击“开始”→“运行”，输入 cmd，单击“确定”按钮。

在出现的命令提示符窗口中输入“ipconfig /all”，回车，即可看到所获得的 IP 地址，如图 3-12 所示。

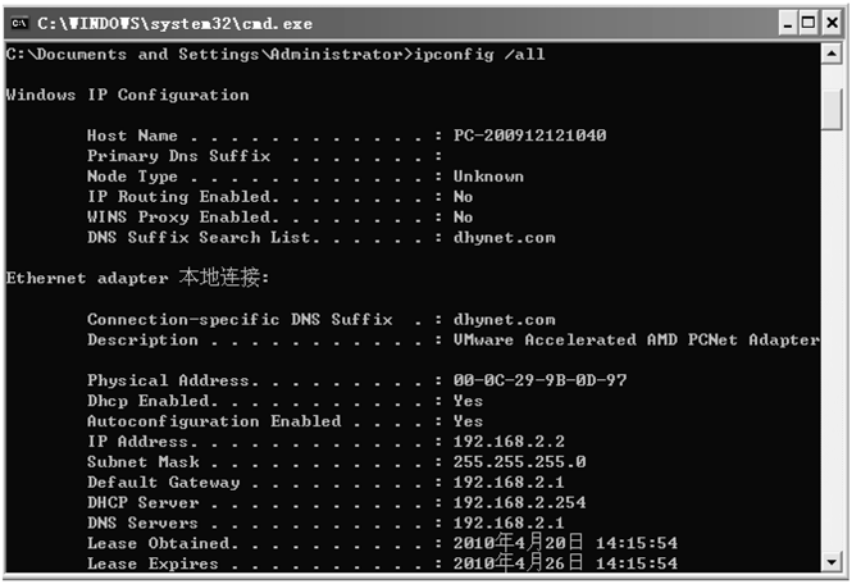

图 3-12　客户端获得 IP 地址情况

同时，在 DHCP 服务器上，我们也能看到 IP 分配情况，如图 3-13 所示。

图 3-13　DHCP 服务器上的 IP 分配情况

3.3.3　任务 3：作用域选项的修改

1．案例分析

现在，你已经完成了自动分配 IP 的配置任务，客户端已经可以自动获取相关 IP 信息及其他相关信息了。如果由于网关 IP 变化或 DNS 服务器 IP 变化，需要重新发布这些信息，需要如何做呢？这个功能，要由 DHCP 中的作用域选项来完成。

2．实施过程

单击“开始”，运行“管理工具”下的“DHCP”，打开 DHCP 服务器管理界面。在 DHCP

服务器管理界面中，单击服务器前“+”号，展开服务器列表，再依次展开“IPv4”和其下的“作用域”前的“+”号，单击“作用域选项”，如图 3-14 所示。

图 3-14　作用域选项信息

在右侧窗格中双击“003 路由器”（即网关）或“006DNS 服务器”，在出现的对话框中，根据需要进行修改，如将路由器地址改为 192.168.2.249，再单击“确定”按钮，如图 3-15 所示，即完成了对相关作用域选项的设定。

图 3-15　设置路由器（网关）信息

3.3.4　任务 4：配置 DHCP 客户端保留

1．案例分析

完成了所有客户端的需求，你还要完成 Web 服务器和 FTP 服务器的 IP 需求。Web 服务器和 FTP 服务器需要每次都获得同一个 IP 地址，并且固定为 192.168.2.66 和 192.168.2.88。在 DHCP 服务器中，可以使用客户端保留来完成这个功能。它的工作原理是将 IP 地址与客户端的网卡 MAC 地址进行绑定，从而达到指定的 IP 地址专门留给特定计算机使用的目的。

2．实施过程

（1）在 DHCP 服务器管理界面中，右击“保留”，在弹出的菜单中，单击“新建保留”命令。

（2）在弹出的“新建保留”对话框中的“保留名称”中，输入此保留的名称，即保留给谁用。此处输入“WEB 服务器”。

（3）在“IP 地址”中，输入要保留的 IP 地址 192.168.2.66。

（4）在“MAC 地址”中，输入 Web 服务器的机器网卡 MAC 地址（关于 MAC 地址的查看方法请参阅相关说明）。“支持的类型”保持默认的“两者”即可，如图 3-16 所示。单击“添加”按钮。

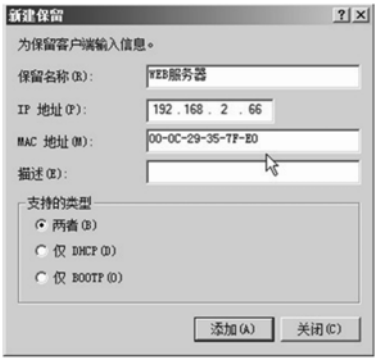

图 3-16　Web 服务器的保留 IP

用同样的方法，为 FTP 服务器添加保留 IP。完成后，Web 服务器和 FTP 服务器的计算机 IP 地址将永久固定为 192.168.2.66 和 192.168.2.88，如图 3-17 所示。

图 3-17　保留 IP 配置后

本项目提出的需求，经过分析后，需要达到以下目的。

- 客户端能够自动获取 IP 地址。
- 在获取 IP 地址的同时，还要能获得网关及 DNS 的配置信息。
- Web 服务器和 FTP 服务器需要获得固定的 IP 地址，即便是重启，也要保证获得的 IP 地址不变，且这两个 IP 地址不能被分配给其他客户端使用。

为了完成项目的需求，我们安装了 DHCP 服务器，配置了 IP 地址池（满足 IP 分配），配置了作用域选项（满足网关和 DNS 配置需求），并对 Web 服务器和 FTP 服务器的 IP 地址进行了保留配置，使它们的 IP 地址每次都能获得固定的一个。

从实际检验结果来看，我们已经达到了项目需求所要求的目标。

3.4　知识能力拓展

3.4.1　DHCP 冗余

1．场景实例

在一个网络中，有 200 台计算机，IP 地址由 DHCP 服务器提供。有一天，DHCP 服务器发生故障，导致所有的计算机都无法获得 IP 地址，无法正常使用网络。为了避免类似的事情发生，你需要做什么？

2．分析

一个 DHCP 服务器故障了，那么我们可以多设定一个 DHCP 服务器，当主 DHCP 服务器故障后，另一个 DHCP 服务器会自动接管。在相同子网上使用多个 DHCP 服务器为 DHCP 客户端服务将提供更强的容错能力。在有两个 DHCP 服务器的情况下，如果一个服务器不可用，那么另一个服务器可以取代它并继续租用新的地址或续订现有客户端。

在两个 DHCP 服务器之间平衡单个网络和地址作用域范围的通常做法是让一个 DHCP 服务器分配 80%的地址，而剩余的 20% 则由第二个服务器提供。

3．实施过程

这个过程很简单，就是再配置一台 DHCP 服务器的过程，不过对于两台 DHCP 服务器的 IP 地址范围有了一些变化。由于配置 DHCP 的过程我们都掌握了，这里不再说明。关于两个 DHCP 服务器的 IP 地址范围设定，请参考图 3-18 进行。需要注意的是，在主 DHCP 服务器上设置的作用域选项，在第二个 DHCP 服务器配置时也要进行同样的设置。

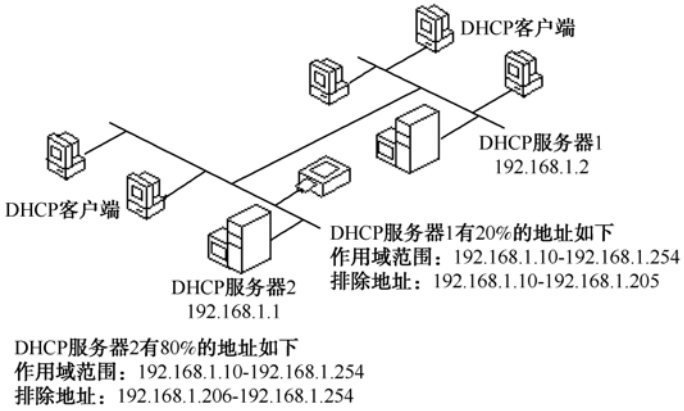

图 3-18　DHCP 冗余配置

3.4.2　DHCP 中继代理的设置

伴随着局域网规模的逐步扩大，一个网络常常会被划分成多个不同的子网，以便根据不同子网的工作要求来实现个性化的管理要求。考虑到规模较大的局域网一般会使用 DHCP 服务器来为各个工作站分配 IP 地址，不过一旦局域网被划分成多个不同的子网时，我们是不是也必须在各个不同的子网中分别创建 DHCP 服务器，来为每一子网中的工作站提供 IP 地址分配服务呢？如果是这样的话，不但操作麻烦，而且还不利于网络的高效管理。其实，我们只要启用

Windows 服务器系统内置的 DHCP 中继代理功能，完全可以将原先的 DHCP 服务器利用起来，分别为多个不同子网提供 IP 地址分配服务。下面，以一台 DHCP 服务器同时为两个子网提供地址分配服务为例，来介绍一下如何利用 DHCP 中继代理程序，给不同子网中的工作站完成跨子网申请 IP 地址的任务。

工作原理如图 3-19 所示，DHCP 服务器在子网 1 中，子网 2 中的 DHCP 客户端 B 和 DHCP 客户端 C 需要获得 IP 地址，则在路由器（由 Windows Server 2008 承担）上启用 DHCP 中继代理功能，即可将子网 2 中的 DHCP 请求转发到子网 1 中的 DHCP 服务器上，从而获得 IP。

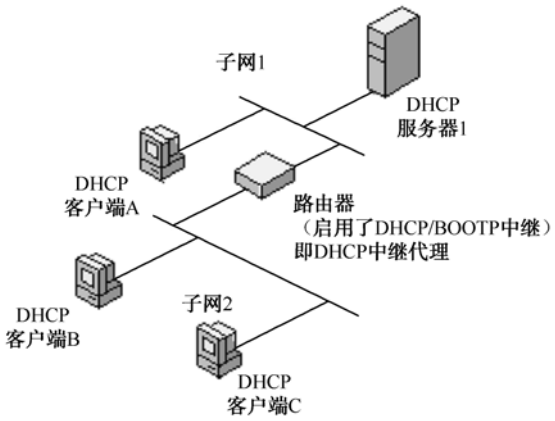

图 3-19　DHCP 中继代理工作原理

实现过程如下。

1．安装路由和远程访问功能（此功能需要两块网卡，以用于两个网段的连接）

（1）单击“开始”，运行“管理工具”下的“服务器管理器”，在“服务器管理器”窗口中，单击“角色”，在右侧窗口中，单击“添加角色”，在出现的“选择服务器角色”中，勾选“网络策略和访问服务”选项，如图 3-20 所示，单击“下一步”按钮。

图 3-20　选择服务器角色

（2）在“选择角色服务”中，勾选如图 3-21 所示的选项，单击“下一步”按钮。

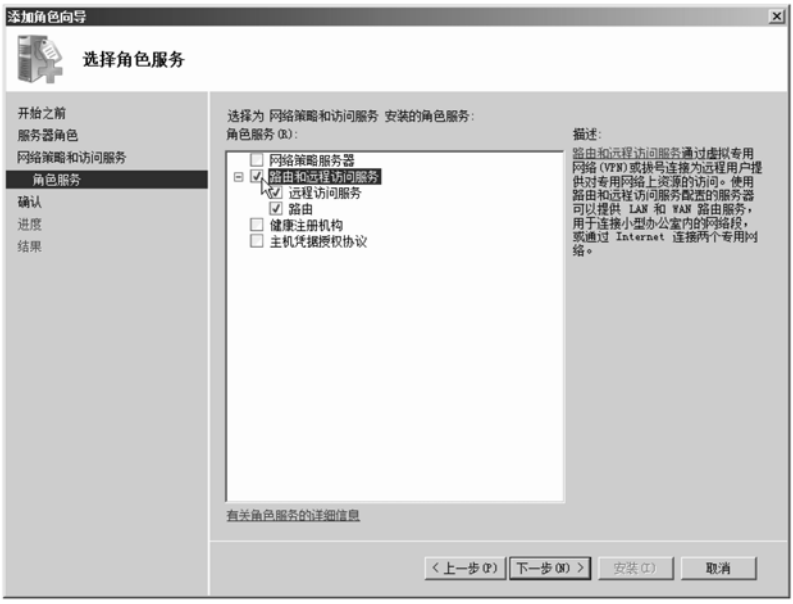

图 3-21　选择角色服务

（3）在出现的“确认安装选择”中，确认所选无误，单击“安装”按钮，最终出现安装成功的提示，单击“关闭”按钮即可。

2．配置远程和路由访问

（1）单击“开始”，运行“管理工具”下的“路由和远程访问”，在出现的“路由和远程访问”窗口中，右击服务器，在弹出的菜单中选择“配置并启用路由和远程访问”，如图 3-22 所示。

图 3-22　配置并启用路由和远程访问

（2）在出现的向导对话框中，单击“下一步”按钮，选择“自定义配置”选项，如图 3-23 所示。

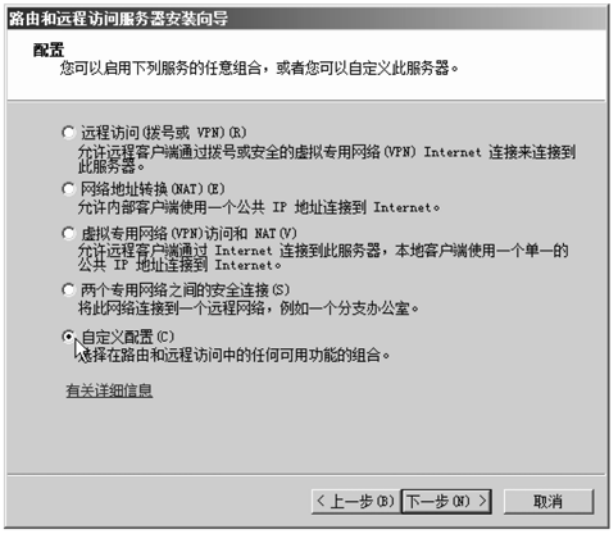

图 3-23　选择自定义配置

（3）单击“下一步”按钮，在其后出现的向导窗口中选中“LAN 路由”复选项，如图 3-24 所示，单击“下一步”按钮，再单击“完成”按钮退出路由和远程访问服务器安装向导窗口，最后在出现的对话框中单击“启动服务”按钮。

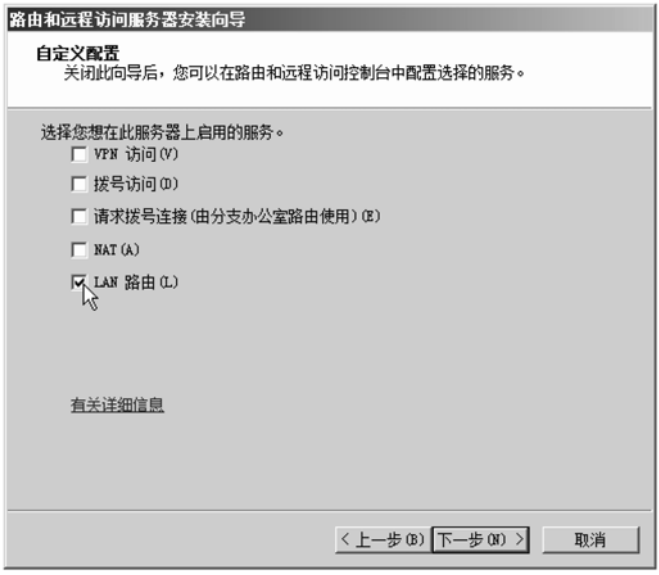

图 3-24　选择“LAN 路由”类型

（4）在出现的“路由和远程访问”管理界面中，单击服务器前的“+”号，再单击“IPv4”前的“+”号，右击出现的“常规”项，在弹出的菜单中单击“新增路由协议”，如图 3-25 所示。

图 3-25　新增路由协议

（5）在出现的对话框中，选择“DHCP 中继代理”，单击“确定”按钮，即完成了 DHCP 中继代理程序的安装。

3．设置 DHCP 中继代理转发器

设置 DHCP 中继代理转发器，让中继代理知道要把 DHCP 转发到哪个 DHCP 服务器上。

（1）右击“DHCP 中继代理程序”，在弹出的菜单中选择“属性”命令。

（2）在“服务器地址”中填入 DHCP 服务器的地址，如 192.168.2.253，单击“添加”按钮，如图 3-26 所示，最后单击“确定”按钮，即完成了 DHCP 代理程序的设置。

图 3-26　设置 DHCP 中级代理的转发信息

（3）新增端口，让 DHCP 中继程序工作于制定的网络端口（即某个网段）上。右击“DHCP 中继代理程序”，在弹出的菜单中执行“新增接口”命令，如图 3-27 所示。

图 3-27　新增中继代理接口

（4）在出现的对话框中，选择需要中继的网段所连接的网卡（即“本地连接”或“本地连接 2”，具体要看需要中继的网段连接的是哪个网卡），单击“确定”按钮。

至此，DHCP 中继代理的设置全部完成，没有 DHCP 服务器的网段的机器，也可以跨网段获取 IP 地址信息了。

3.5　项目完成结论

在本项目的案例中，学习了安装 DHCP 服务器，并按不同需求配置 DHCP 服务器的方法，如客户端能够自动获取 IP 地址，并在获取 IP 地址的同时，还要能获得网关的 DNS 的配置信息。Web 服务器和 FTP 服务器需要获得固定的 IP 地址，即便是重启，也要能保证获得的 IP 地址不变，且这两个 IP 地址不能被分配给其他客户端使用。在知识拓展部分，还对 DHCP 冗余和 DHCP 中继代理进行了讲解，以满足不同环境要求的需要。

3.6　练习案例

你是 test.net 公司的网络管理员，该公司的外联部门有 30 个员工，要组成工作组模式。你为了减少配置 IP 地址的工作量，计划让所有客户端自动获得 IP 地址。并且，外联部通过网关 192.168.0.100 进行外网访问，并同时使用 192.168.0.100 进行 DNS 查询，你希望所有员工的客户机能够在自动获得 IP 地址的时候，同时获得网关和 DNS 的配置信息。另外，希望流媒体服务器的 IP 地址不要变动，在自动获取后，也总是保持 192.168.0.1，你要如何解决？

3.7　课后习题

1. 公司原有一个网络，网段地址是 192.168.2.0/24，这些地址是由 Windows Server 2008 的 DHCP 服务器分配的。现因公司规模扩大，增加了一个子网，新子网与原有子网之间通过路由器连接。管理员配置新子网的客户机通过 DHCP 服务器获取 IP 地址。但发现新子网上的客户

机无法从 DHCP 服务获取 IP 地址，而原来的子网中的客户机没有这个问题。你认为是什么原因？（　　）

A．原来的 DHCP 作用域的地址池中的 IP 地址已经分配完了

B．DHCP 服务器的作用域没有被激活，因此不能分配 IP 地址

C．连接两个子网所使用的路由器不支持客户机的 DHCP 广播

D．路由器配置不正确

2．一个公司网络中，有一台 DHCP 服务器进行 IP 地址分配，所有客户端都是从 DHCP 服务器获取 IP 地址的，网段为 192.168.1.0/24。公司新近招收了一批员工，并配备了计算机，管理员告诉他们，将计算机设置为 DHCP 客户端即可获取 IP 地址。但他们中的几个人说无法获得 IP 地址，系统提示网络受限，其余的人没有这个问题，而且，查看提示网络受限的用户的客户端 IP 地址，发现他们的 IP 为 169.254.0.0/24。可能的原因是什么？（　　）

A．DHCP 服务器地址池中的 IP 地址全部分配完了，不能再提供 IP 地址

B．没有把客户端设置为 DHCP 客户端

C．客户端计算机网线故障

D．以上都不是

3．你是公司的网络管理员，公司里的客户端使用的操作系统为 Windows XP，并设置为 DHCP 客户端。公司有一个主办公室和一个分办公室，两个办公室由一个路由器分开，每一个办公室配置了一个 DHCP 服务器。

其中的一个 DHCP 服务器意外关闭了，维修服务器使用了 4 个小时。在这段时间内，许多移动用户将他们的便携式电脑连接至网络并发现他们不能连接网络上的共享资源。在服务器维修好之后，你在每个 DHCP 服务器上创建了一个包含另外一个办公室 IP 地址的新的作用域，以便再次出现某一台 DHCP 服务器故障时，另一台可以接替故障服务器继续提供服务。你关闭了主办公室的 DHCP 服务器来测试新的 DHCP 服务器，发现主办公室内的客户端计算机不能从分办公室的 DHCP 服务器上接收到 IP 地址，你需要确认当一个办公室里的 DHCP 服务器失效时，客户端计算机可以从另一个办公室接收到正确的 IP 地址。请选出正确答案（　　）。（答案有两个）

A．设置办公室之间的路由器，使其支持 BOOTP 式的广播

B．设置每个办公室内的 DHCP 服务器，使其拥有一个包含着另外的一个办公室的 IP 地址的 DHCP 作用域，并激活这个作用域

C．利用另外的网络适配器来设置每个办公室的 DHCP 服务器，将每个新的网络适配器连接至本地网络。从每个办公室的网络中分配一个新的 IP 地址至新的网络适配器

D．安装和设置一个 DHCP 传播代理到每个办公室

4．简述 DHCP 服务器的工作原理。

5．由 DHCP 服务器提供 IP 地址给客户机，相比手动设置客户机 IP 地址有什么好处？

6．DHCP 服务器安装前，必须为该服务器设置固定 IP 地址吗？为什么？请用自己的话进行概括。

7.某公司内部使用 DHCP 服务器进行 IP 地址管理，现希望内部的流媒体服务器能从 DHCP 服务器获取一个固定的 IP，且该 IP 不会与其他机器产生冲突，需要使用哪种功能？请概述如何进行设置。

项目 4　DNS 服务器的安装、配置与管理

网络解决方案需要纳入域名系统（DNS）来连接网络基础设施的各个组件。将主机名解析为 IP 地址的过程是连接组件的重要因素。本章的主要目的是概要说明 Windows Server 2008 网络基础架构中域名服务器的配置，了解如何在企业内部配置域名服务器，如何配置 DHCP 服务器和 DNS 服务器的混合使用，掌握 DNS 区域设置，以及常见 DNS 服务器注意事项。希望大家能够掌握以上知识点，并且通过本项目的讨论和学习掌握相关的网络环境。

知识点、技能点

- 掌握 DNS 在网络基础设施中的作用
- 能够安装 DNS 服务器
- 能够配置 DNS 服务器服务属性
- 能够配置 DNS 区域
- 能够配置 DNS 区域复制
- 能够配置动态更新
- 能够配置 DNS 客户端

4.1　引例：为什么要使用 DNS 服务器（WHY）

在 Internet 中，内容提供商将其信息以网站的形式展现给用户，而整个因特网的网站都是以一台一台服务器的形式存在的，但是我们怎么去找到要访问的网站服务器呢？这就需要给每台服务器分配 IP 地址，我们可以通过访问一个 IP 地址的形式去访问一个网站，但是因特网上的网站难以计数，我们很难记住所有的网站，甚至是非常细微的一小部分都有难度。那么如何解决这种问题呢？

为了解决记忆大量网站 IP 地址的问题，产生了方便记忆的域名管理系统 DNS（域名服务系统），它可以把我们输入的好记的域名转换为要访问的服务器的 IP 地址。简单地说，就是可以方便我们浏览因特网上的网站，不用去刻意记住每个主机的 IP 地址。DNS 服务器提供的就是将域名解析为 IP 的服务，从而使我们上网的时候能够用简短而好记的域名来访问因特网上的静态 IP 的主机。

4.2　案例 1：DNS 服务器的基本配置

4.2.1　工作情景描述

DHYNET 是国内知名电子产品生产企业，公司主要生产移动存储设备、MP3、MP4、显卡、主板等电子产品。公司正处与快速成长期，在 2～3 年中。人员规模从原先仅 100 人的团队，迅速扩张为现在的 800 人规模。随着公司规模的扩张，公司加快了信息化建设及管理的步伐，先后购置了 10 台服务器，其中网站服务器 1 台，邮件服务器 3 台，内部 OA 服务器 1 台，FTP 服务器 1 台。公司很多业务都是基于 B/S 系统的，相应的处理服务器有 4 台。同时为了公

司对外交流的应用，公司申请了 dhynet.com 的域名，为了更好地进行集中化的管理，公司决定采用基于 Windows 活动目录的管理方式。同时公司要求做到如下几点。

（1）能为公司员工提供尽可能简单的方法访问公司的应用系统（大部分是以 Web 网站的形式），当对内提供服务的服务器更换 IP 地址的时候，所花的代价最小。

（2）为了管理的方便，公司需要使用主机名字进行相互的资源访问。

（3）应该能够根据 IP 地址情况查找到相应的计算机的名字。

（4）公司内部的 Web 服务器名称为 www.dhynet.com，对应的内部地址为 10.0.0.100，FTP 服务器名称为 ftp.dhynet.com，对应的内部地址也为 10.0.0.100，邮件服务器为 email.dhynet.com，对应的内部地址为 10.0.0.102，OA 服务器的名称为 OA.dhynet.com，对应的内部地址为 10.0.0.103。域控制器的地址为 10.0.0.1。

（5）公司每天都有大量的邮件需要处理，邮件服务也是公司最主要及最为繁重的业务，为了保证快速的响应及可靠性，公司目前共设立了 2 台邮件服务器，名称分别为 win2k2.dhynet.com 和 win2k3.dhynet.com，对应的 IP 地址分别为 10.0.0.104 和 10.0.0.105，并且当 win2k2 无法联系的时候会自动切换到 win2k3 上工作。

4.2.2　案例分析

（1）在本项目中，该公司为了更好地进行集中化的管理，公司决定采用基于 Windows 活动目录的管理方式。在网络中必须安装 DNS 服务器。

（2）能为公司员工提供尽可能简单的方法访问公司的应用系统（大部分是以 Web 网站的形式）；当对内提供服务的服务器更换地址的时候，花的代价最少；为了管理的方便，公司还需要使用主机名字进行相互的资源访问；应该能够根据 IP 地址情况查找到相应的计算机的名字。要实现这些，就必须要使用 DNS 服务器的区域及主机资源记录的内容。

（3）因为该公司每天都有大量的邮件需要处理，需要构建邮件服务，为了保证快速的响应及可靠性，公司需要设立 2 台邮件服务器，需要对其进行设置。

4.2.3　相关知识

为了解决上述场景中的问题，首先有必要对 DNS 服务的相关概念有一个整体的了解。

1．域名和计算机名称

域名是企业、政府、非政府组织等机构或者个人在因特网上注册的名称，是因特网上企业或机构间相互联络的网络地址。例如，经常看到的 aaa.bbb.com 这类的名称，这就是一个完全合格的域名，也被称为 FQDN。该名称描述了一台主机所属的网络位置。它同一个或几个 IP 地址相互对应。这个与网络上的数字型 IP 地址相对应的字符型地址，就被称为域名。DNS 服务的作用就是将难以记忆的 IP 地址同域名进行相互解析。这样网络上的资源访问起来就容易得多了。

计算机名称又称为 NETBIOS 名称，是 FQDN 中最左边的部分，也是安装操作系统时为计算机起的名字，用来指定 Internet 或企业网络中的专用计算机。

2．域名空间结构

为了更方便、快捷地定位到连接 Internet 上的一台计算机，域名采用层次型结构。从而可以将因特网上难以计算的计算机的 IP 及域名分别保存在不同的 DNS 服务器上，采用这种分层的结构，大大地加快了 DNS 名称解析的速度。在 DNS 中，域名的层次结构包括根域、顶级域、

二级域、下属子域和主机等。该层次结构类似于一棵倒置的树，最上边的树根就是顶级域，往下依次是二级域、三级域等，而树叶就是计算机，如图 4-1 所示。

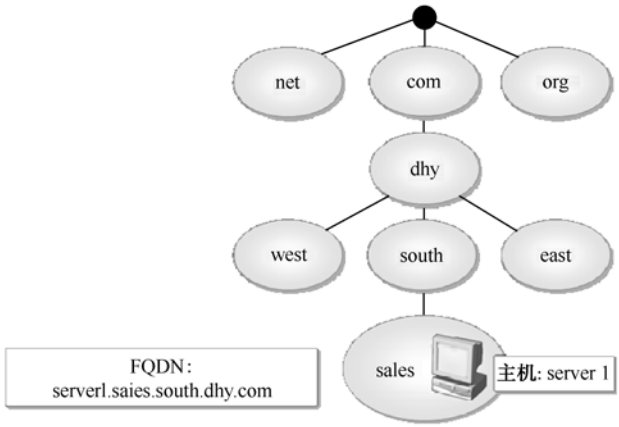

图 4-1　域名空间的层次结构

图 4-1 最上边的黑点代表根域，由国际互联网络信息中心（Inter NIC）负责管理，该机构把域名空间各部分的管理职责分配给连接到 Internet 的各个组织。

顶级域名又分为两类：一是国家顶级域名（National Top-Level Domainnames，nTLDs），目前 200 多个国家都按照 ISO3166 国家代码分配了顶级域名，如中国是 cn，美国是 us，日本是 jp 等；二是国际顶级域名（International Top-Level Domainnames，iTDs），如表示工商企业的.com，表示网络提供商的.net，表示非营利组织的.org 等。

二级域名是指顶级域名之下的域名，在国际顶级域名下，它是指域名注册人的网上名称，如 ibm、yahoo、microsoft 等；在国家顶级域名下，它是表示注册企业类别的符号，如 com、edu、gov、net 等。在该二级域名中，各公司或个人也可根据各自的情况划分下级子域或主机等，如注册 dhynet.com 后，可在该二级子域下建立子域 south.dhynet.com 等。

主机名称就是 FQDN 中最左边的部分，代表某一个组织或公司内部的具体某一台主机。

3．域名查询过程

查询是个说简单也简单，说复杂也复杂的过程，但是它一定会对系统性能造成非常大的影响。一般情况下，当客户机发起域名方式访问某台主机的时候，DNS 服务器必须解决域名到 IP 地址转换的问题，由于 DNS 域名空间是一个层次型的结构，因此可能需要 DNS 服务器同 Internet 上的其他 DNS 服务器共同完成一个域名的查找过程，具体来说域名查询可以分为以下两种类型。

1）*递归查询*

递归查询是最常见的查询方式，域名服务器将代替提出请求的客户机（下级 DNS 服务器）进行域名查询，若域名服务器不能直接回答，则域名服务器会在域各树中的各分支的上下进行递归查询，最终将查询结果返回给客户机，在域名服务器查询期间，客户机将完全处于等待状态。当收到 DNS 工作站的查询请求后，DNS 服务器在自己的缓存或区域数据库中查找，如找到则返回结果，如找不到，则返回错误结果。即 DNS 服务器只会向 DNS 工作站返回两种信息，要么是在该 DNS 服务器上查找到的结果，要么是查询失败。该 DNS 工作站自行向该 DNS 服务器询问。“递归”的意思是有来有往，并且来往的次数是一致的。一般由 DNS 工作站提出的查询请求便属于递归查询。

2）迭代查询

在迭代查询中，虽然一个 DNS 服务器可能不知道某个域名下记录的 IP 地址，但它可能知道管理具有要找的 IP 地址名字的服务器的 IP 地址，于是它将信息发给客户端，由客户端再到这个 IP 地址进行寻找。对一个迭代查询的响应就像一个 DNS 服务器在说：“我不知道你找的 IP 地址是多少，但是我知道位于 4.1.2.3 的域名服务器可以告诉你。”这个过程很简单。你把它理解成为推卸责任也可以。你可以根据 DNS 服务器的具体性能考虑选择哪种查询方式，通常我们在小型企业中选择迭代查询，因为这样可以减小服务器的压力。

当 DNS 客户端需要查询程序中使用的名称时，它会查询 DNS 服务器来解析该名称。客户端发送的每条查询消息都包括以下 3 条信息。

- 指定服务器回答的问题。
- 指定的 DNS 域名，规定为完全合格的域名（FQDN）。
- 指定的查询类型，可根据类型指定资源记录，或者指定查询操作的专用类型。

例如，指定的名称可为计算机的 FQDN，如 host-a.example.microsoft.com，并且指定的查询类型用于通过该名称搜索地址（A）资源记录。将 DNS 查询看做客户端向服务器询问由两部分组成的问题：“您是否拥有名为‘hostname.example.microsoft.com’的计算机的 A 资源记录？”当客户端收到来自服务器的应答时，它将读取并解释应答的 A 资源记录，获取根据名称询问的计算机的 IP 地址。

DNS 查询以各种不同的方式进行解析。有时，客户端也可使用从先前的查询获得的缓存信息在本地应答查询。DNS 服务器可使用其自身的资源记录信息缓存来应答查询。DNS 服务器也可代表请求客户端查询或联系其他 DNS 服务器，以便完全解析该名称，并随后将应答返回至客户端。这个过程称为递归。

另外，客户端自己也可尝试联系其他的 DNS 服务器来解析名称。当客户端执行此操作时，它会根据来自服务器的参考答案，使用其他的独立查询。这个过程称为迭代。

总之，DNS 查询进程分两部分进行。

- 名称查询从客户端计算机开始，并传输至解析程序，即 DNS 客户端服务程序进行解析。
- 不能在本地解析查询时，可根据需要查询 DNS 服务器来解析名称。

如图 4-2 所示显示了完整的 DNS 查询进程的概况。

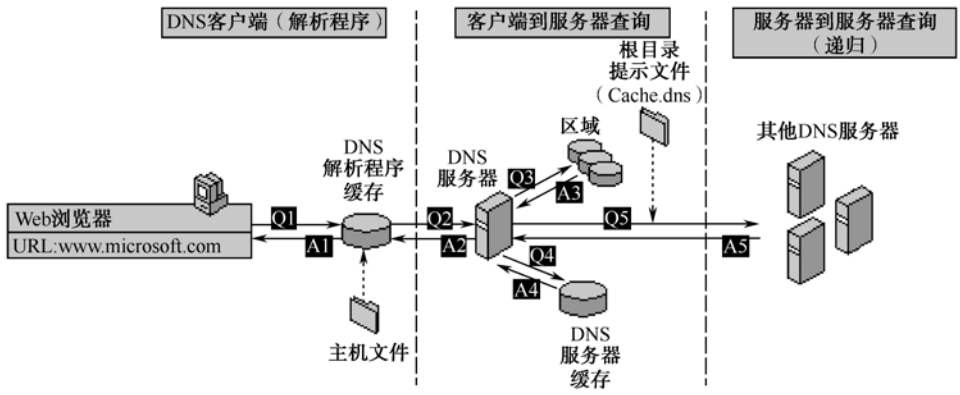

图 4-2　DNS 查询过程

下面将更加详细地解释这两个过程。

如查询过程的初始步骤所示，DNS 域名由本机的程序使用。该请求随后传输至 DNS 客户端服务，以便使用本地缓存信息进行解析。如果可以解析查询的名称，则应答该查询，该进程完成。

本地解析程序的缓存可包括从两个可能的来源获取的名称信息。

- 如果在本地配置主机文件，则来自该文件的任何主机名称到地址的映射，在 DNS 客户端服务启动时将预先加载到缓存中。从以前的 DNS 查询应答的响应中获取的资源记录，将被添加至缓存并保留一段时间。
- 如果此查询与缓存中的项目不匹配，则解析过程继续进行，客户端查询 DNS 服务器来解析名称。

如图 4-3 所示，客户端将查询首选 DNS 服务器。在此进程的初始客户端/服务器查询部分中使用的实际服务器选自全局列表。

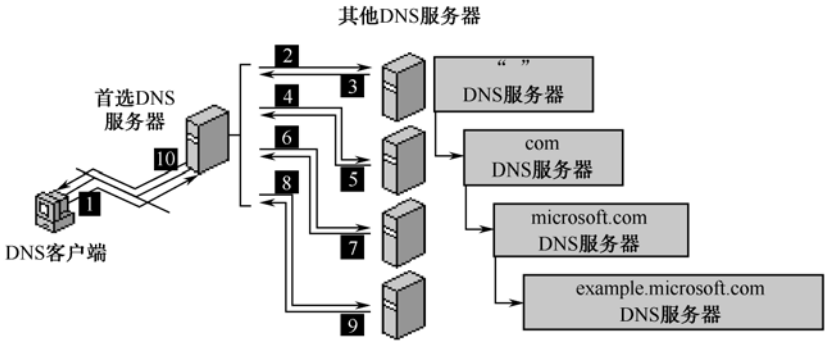

图 4-3　查询 DNS 服务器

使用根提示查找根服务器，DNS 服务器可完成递归的使用。理论上，该进程将启用 DNS 服务器，以定位那些对域命名空间树的任何级别使用的任何其他 DNS 域名具有绝对控制权的服务器。

例如，当客户端查询单个 DNS 服务器时，考虑使用递归过程来定位名称 host-b.example.microsoft.com。在 DNS 服务器和客户端首次启动，并且没有本地缓存信息可帮助解析名称查询时，就会进行上述过程。根据其配置的区域，它假定由客户端查询的名称是域名，该服务器在本地不包含有关该域名的信息。

首先，首选服务器分析全名并确定对于顶级域“com”具有绝对控制权的服务器的位置。其次，对“com”DNS 服务器使用迭代查询，以获取“microsoft.com”服务器的参考信息。然后，参考应答从“microsoft.com”服务器传送到“example.microsoft.com”的 DNS 服务器。最后，与服务器 example.microsoft.com 建立联系。因为该服务器包括作为其配置区域一部分的查询名称，所以它向启动递归的源服务器做出权威性地应答。当源服务器接收到表明已获得对请求查询的权威性应答的响应时，它将此应答转发给发出请求的客户端，这样递归查询过程就完成了。

尽管执行上述递归查询过程可能需要占用大量资源，但对于 DNS 服务器来说它仍然具有一些性能上的优势。例如，在递归过程中，执行递归查询的 DNS 服务器可获得有关 DNS 域命名空间的信息。该信息由服务器缓存起来并可再次使用，以便提高使用此信息或与之匹配的后续查询的应答速度。随着时间的推移，这些缓存信息会不断增加并占据大量的服务器内存资源，尽管每次 DNS 服务重新启动时这一信息将被清除。

4.3　案例 1 实施过程

在掌握了基本的 DNS 服务器的相关知识之后，我们来完成案例 1 的内容。

4.3.1　任务 1：DNS 服务器的安装及配置过程

1．案例分析

为了更好地进行集中化的管理，公司决定采用基于 Windows 活动目录的管理方式，所以必须要有 DNS 的支持。这一点我们前面已经提到过，域控制器建立的时候，需要 DNS 服务器为域中的计算机提供服务的查询，即域控制器要在活动目录中注册相应的 SRV 记录，以便客户机通过 DNS 查找到在该域内提供 kerberos 验证的服务器地址。

2．实施过程

在实际企业场景中配置 DNS 服务器一定要进行事先的规划，经过相关批准和审核才能进行进一步的安装，因为随意的安装域名服务器可能导致企业内部的名称解析混乱。同时，作为 DNS 服务器的计算机必须预先安装 Server 版的操作系统及采用静态的 IP 地址配置，在此建议采用 Windows Server 2008 企业版。为了保证 DNS 服务器能够正常地对外提供服务，事先必须进行相关的文档准备，记录 DNS 服务器的 IP 地址等信息，为日后企业的规范化信息管理打下基础。

3．DNS 服务器的安装

我们已经选定了一台安装了 Windows Server 2008 企业版的计算机作为我们的 DNS 服务器，同时由于 DHYNET 公司采用 AD 的集中管理方式，为了实现更高的安全性管理，在这里我们将活动目录服务器同 DNS 服务器进行集成操作，即在建立活动目录域的同时安装 DNS 服务，而为了区别起见，我们将单独进行演示。

（1）如图 4-4 所示，将计算机的 IP 地址设置为 10.0.0.1，并完成相应“子网掩码”及“首选 DNS 服务器”的设置。

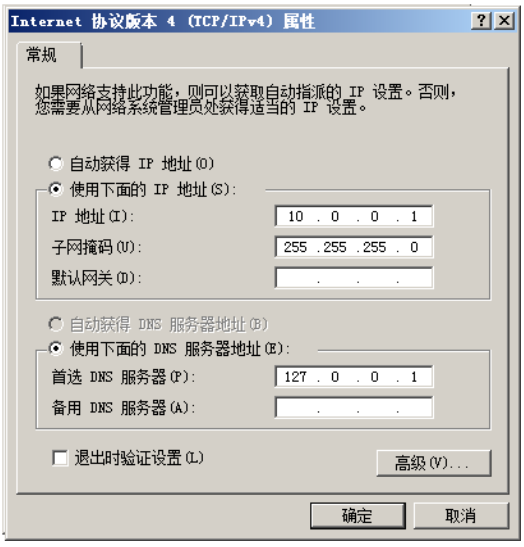

图 4-4　IP 地址的设置

（2）单击“开始”按钮，选择“管理工具”→“服务器管理器”，如图 4-5 所示。

图 4-5　打开“服务器管理器”

（3）在“服务器管理器”对话框中，单击“角色”，如图 4-6 所示。

图 4-6　“服务器管理器”对话框

（4）在右侧的“角色摘要”处单击“添加角色”，在弹出的“添加角色向导”对话框中，勾选“DNS 服务器”选项。然后单击“下一步”按钮，如图 4-7 所示。

图 4-7　添加“DNS 服务器”角色

（5）在弹出的对话框中，查看显示内容并单击“下一步”按钮，然后再“确认”步骤中，单击“安装”按钮。接下来进入到添加角色向导的“进度”步骤，等待 DNS 角色安装完成，在添加角色向导的“结果”步骤中，单击“关闭”按钮。在安装完成 DNS 服务后，打开“服务器管理器”对话框，单击“角色”，查看 DNS 服务器是否安装完成，如图 4-8 所示。

图 4-8　查看 DNS 服务器是否安装成功

4．DNS 客户端的设置

DNS 服务器安装完成后，还需要对客户端进行设置，否则不能进行名字解析服务。我们将以 Windows XP Professional 为例，讲授客户端的配置方法。

（1）打开客户端计算机的“Internet（TCP/IP）协议属性”对话框。在“首选 DNS 服务器”位置添加我们刚刚建立的 DNS 服务器的 IP 地址，如图 4-9 所示。

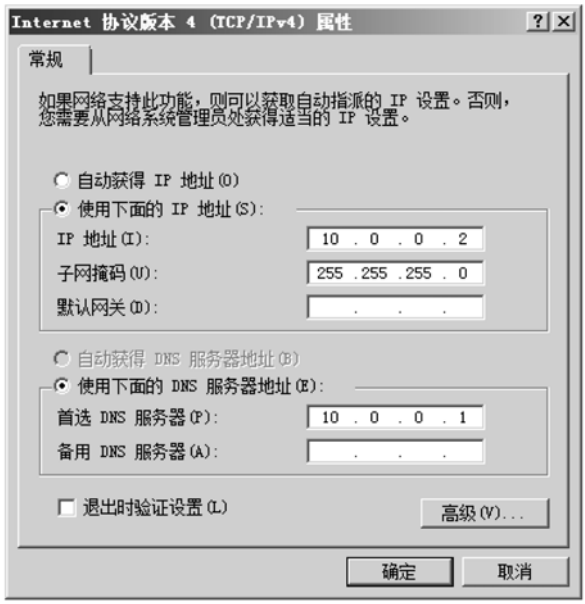

图 4-9　DNS 客户端配置

（2）在企业网络中，一般的服务器都是成对出现的，防止由于单点故障导致网络发生故障的问题。为此，可能设置了额外的 DNS 服务器，那么我们可以在“备用 DNS 服务器”处添加备用 DNS 服务器的 IP 地址。同时可以在图 4-10 中设置更多的可以使用的 DNS 服务器。

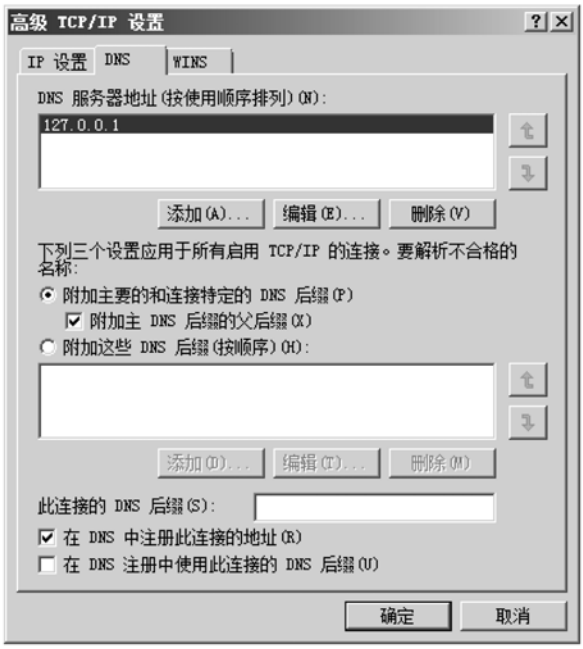

图 4-10　备用 DNS 客户端配置

特别需要注意，只有当主 DNS 服务器不能联系的时候，系统才会去查找备用 DNS 服务器，而不论备用 DNS 服务器是否能够解析。也就是说，当主 DNS 服务器不能对一个域名进

行解析时，尽管备用 DNS 服务器可以解析，但是当主 DNS 服务器可用时，将不会去查找辅助 DNS 服务器。

（3）在客户端计算机的命令提示符下输入 nslookup 命令，来查看是否设置成功。当在 Address 位置出现设置的 DNS 服务器地址 10.0.0.1 的时候，证明已经设置完毕了。由于现在的 DNS 服务器没有做更多的设置，所以无法进行其他的测试，如图 4-11 所示。

图 4-11　DNS 客户端测试

4.3.2　任务 2：区域的建立及建立主机资源记录

1．案例分析

该公司要求能为公司员工提供尽可能简单的方法访问公司的应用系统（大部分是以 Web 网站的形式），当对内提供服务的服务器更换地址的时候，花的代价最少；为了管理的方便，公司还需要使用主机名字进行相互的资源访问；应该能够根据 IP 地址情况查找到相应的计算机的名字。而要实现这些，就必须要使用 DNS 服务器的区域及主机资源记录的内容。

要使用尽可能简单的方法实现公司应用系统的访问，我们需要为各个服务器配置域名，使其域名同 IP 地址有相互对应的关系，这实际上用到了 DNS 服务器最基本的功能。当服务器的 IP 地址发生更改的时候，我们只需要在 DNS 服务器上做一次修改，客户端就可以重新定向到新的 IP 地址的服务器上去，不需要再做额外的任何事情。

要使用名字进行相互资源的访问，需要在 DNS 服务器上建立相应的主机记录。当客户端向服务器提出域名解析的时候，DNS 服务器根据数据库内注册的内容进行解析。

要解决使用 IP 地址查找域名的问题，需要建立相应的反向指针记录。

2．实施过程

建立好 DNS 服务器后，第一步要做的就是创建区域。什么是区域，回顾一下 DNS 的架构图，可以发现区域是域名称空间的一个划分，DNS 服务器对该名称空间解析 DNS 查询时有权威性。可以将 DNS 名称空间划分为区域，这些区域存储一个或多个 DNS 域或部分 DNS 域的名称信息，一个区域对于该区域中包含的每个 DNS 域名是权威的信息来源。创建区域分为创建正向查找区域和反向查找区域。区域类型又分为 3 种类型的区域，即主要区域、辅助区域及存根区域。

- 正向查找区域：根据已知的域名解析相应的 IP 地址。

- 反向查找区域：根据已知的 IP 解析相应的域名。
- 主要区域：用来存储此区域内所有记录的正本。当建立了主要区域后，就可以对该区域内的记录进行添加、修改和删除等操作了，区域内的记录存储在文件或者活动目录数据库中。

如果 DNS 服务器是独立服务器或成员服务器，则区域内的记录将保存在名为“区域名称.dns”的区域文件内，该文件符合标准 DNS 格式，即可以在多种不同的系统内通过更改文件后缀的形式进行简单互换。

如果 DNS 服务器同活动目录服务器进行了集成，那么还可以有另外一种存储的形式，区域内的记录可以存放在活动目录数据库内，随活动目录数据库的复制而自动复制。

- 辅助区域：从某一个主要区域 DNS 服务器复制其区域记录，记录是只读的，不能进行添加及修改的操作，仅仅能提供解析，以分担主要区域 DNS 服务器的解析负担。

例如，test.net 域有 3 台 DNS 服务器负责解析（“>”代表复制方向）：dns01>dns02>dns03。那么，dns01 是主要区域的 DNS 服务器，其记录是可读可写的。dns02 是辅助区域的 DNS 服务器，其记录是只读的，其主控 dns 就是 dns01。dns03 是辅助区域的 DNS 服务器，其记录是只读的，其主控 dns 就是 dns02。

在 Windows Server 2008 DNS 服务的默认配置下，DNS 辅助区域会在无法联系到其主控 DNS 的 24 小时之后，停止域名解析工作。

用一个比喻来说，辅助区域就像经理安排了经理助理，其助理只能分担其工作，但不能代表经理决策。

3．在正向查找区域中创建主要区域

（1）在“服务器管理器”控制台中，选择“角色”中的“DNS 服务器”，打开“DNS”，右击“正向查找区域”，从快捷菜单中选择“新建区域”，如图 4-12 所示。

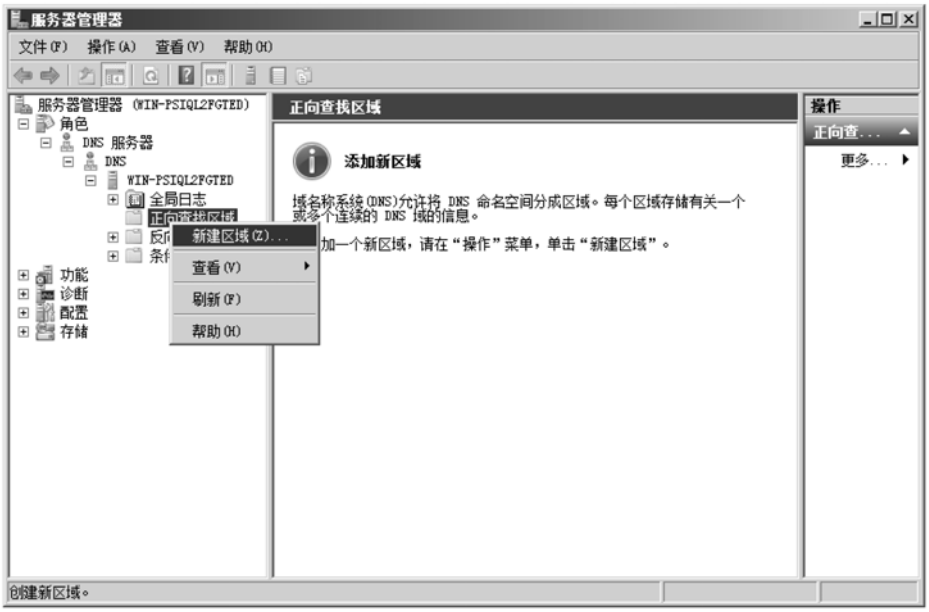

图 4-12　新建区域

（2）在“新建区域向导”对话框中单击“下一步”按钮，并在出现的“区域类型”对话框中选择“主要区域”，然后单击“下一步”按钮，如图 4-13 所示。

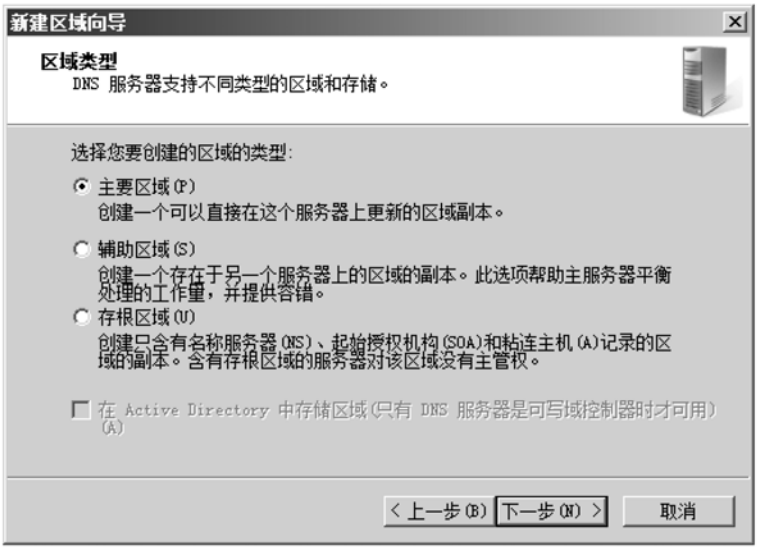

图 4-13　建立“主要区域”

（3）在“区域名称”对话框的“区域名称”文本框中输入 DHYNET 公司的域名 dhynet.com，然后单击“下一步”按钮，如图 4-14 所示。

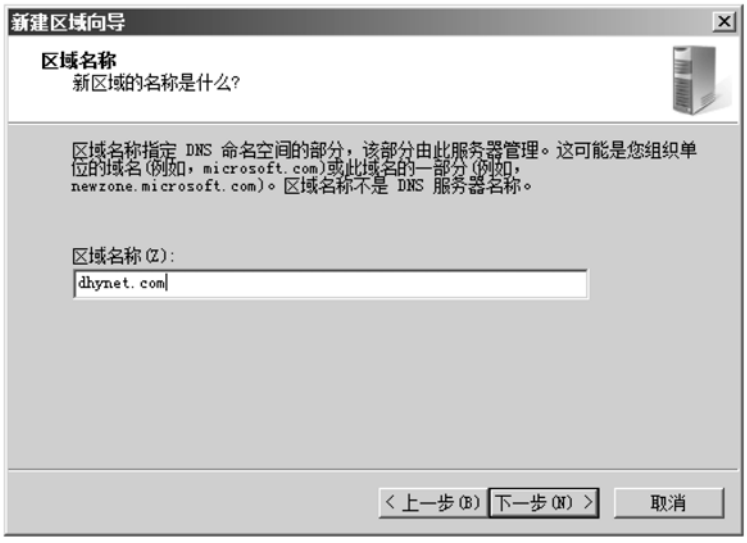

图 4-14　设置“区域名称”

（4）在“新建区域向导”对话框的“区域文件”步骤中，保持默认设置即可，单击“下一步”按钮。如果要使用已有的区域文件，则需要先将该文件复制到“%systemroot%\system32\dns”文件夹内，然后选择“使用此现存文件”，如图 4-15 所示。

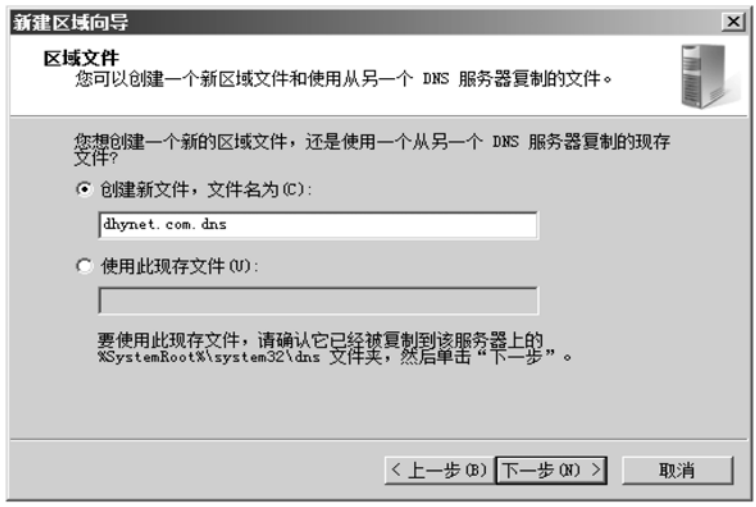

图 4-15　设置“区域文件”

（5）在“新建区域向导”对话框的“动态更新”步骤中设置动态更新属性，此处由于当前 DNS 服务器没有与 AD 进行集成，所以“只允许安全的动态更新”选项为灰色的。为了能够实现多台计算机的自动注册，我们选择“允许非安全和安全动态更新”，并单击“下一步”按钮，如图 4-16 所示。

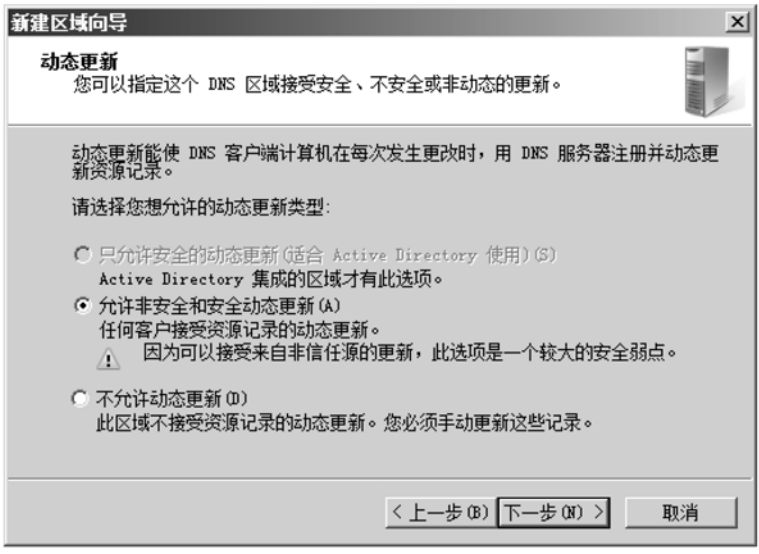

图 4-16　设置“动态更新”

（6）在“新建区域向导”对话框的“正在完成新建区域向导”步骤中，仔细核对所做的设置是否正确，如有问题单击“上一步”按钮返回上级窗口进行重新设定，如果没有问题，单击“完成”按钮，结束主要区域的创建，如图 4-17 所示。

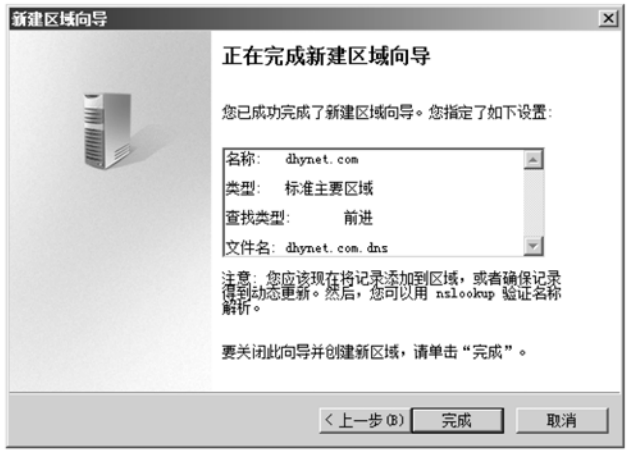

图 4-17　完成正向区域设置

（7）在“服务器管理器”控制台窗口中，查看正向查找区域中是否已经生成了我们建立的主要区域 dhynet.com，如图 4-18 所示。

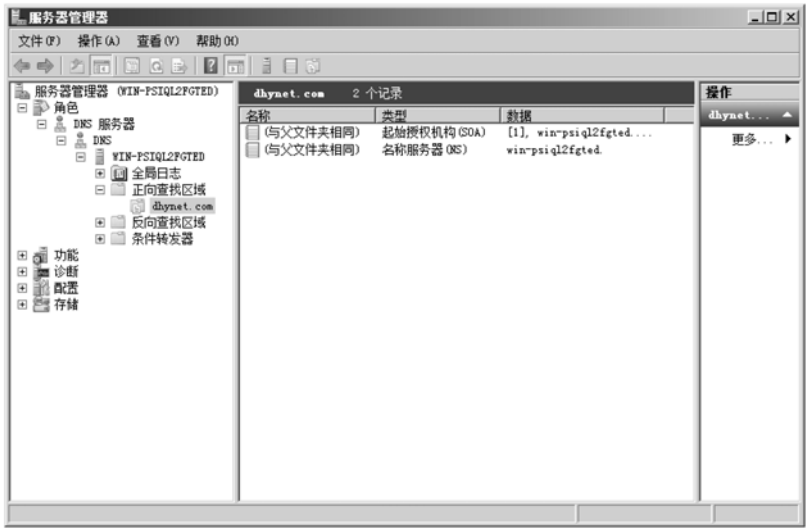

图 4-18　查看正向查找区域

4．在区域中创建相应的资源记录

根据使用场景的不同，DNS 服务器有不同的资源记录类型。常见的有如下几种。

- 主机（A）：用于将 DNS 域名映射到计算机使用的 IP 地址。
- 别名（CNAME）：用于将 DNS 域名的别名映射到另一个主要的或规范的名称。别名资源记录有时也称为规范名称。这些记录允许使用多个名称指向单个主机，使得某些任务更容易执行。例如，在同一台计算机上维护 FTP 服务器和 Web 服务器，建议在下列情况中使用 CNAME 资源记录，即在同一区域的 A 资源记录中指定的主机需要被重新命名时，或当用于像 WWW 这样的已知服务器的通用名称需要解析一组提供相同服务的单独计算机（每个都有单独的 A 资源记录）时，如一组冗余 Web 服务器。
- 邮件交换器（MX）：用于将 DNS 域名映射为交换或转发邮件的计算机的名称。它由电子邮件应用程序使用，用来根据在目标地址中使用的 DNS 域名为电子邮件接收定位邮件服

务器。例如，对名称 example.microsoft.com 的 DNS 查询可能会用于寻找 MX 资源记录，允许电子邮件应用程序转发或交换到电子邮件地址为 user@example.microsoft.com 的用户。

- 指针（PTR）：用于映射基于指向正向 DNS 域名的计算机的 IP 地址的反向 DNS 域名，支持在 in-addr.arpa 域中创建和确立的区域的反向搜索过程。这些记录用于通过 IP 地址定位计算机并将该计算机信息解析为 DNS 域名。

根据任务的要求，需要建立相应的主机记录、别名记录、邮件交换记录及指针记录。

（1）打开“服务器管理器”控制台，选择 DNS 服务器角色，右击区域“dhynet.com”，在弹出的快捷菜单中选择“新建主机”，如图 4-19 所示。

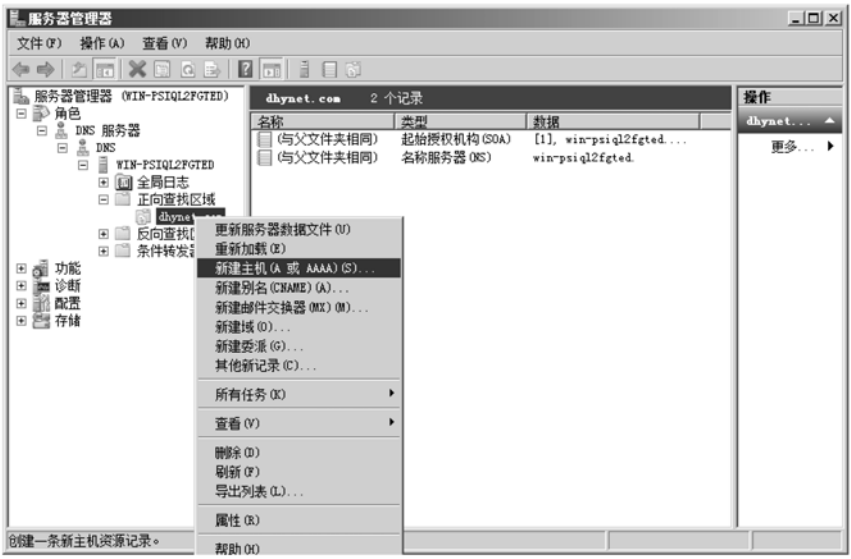

图 4-19　新建主机

（2）在“新建主机”对话框中的“名称”文本框中输入服务器的主机名称 www，“IP 地址”文本框中输入 10.0.0.100，“完全限定的域名”文本框中将自动把主机名添加到域名的最左边，形成 FQDN 的形式。单击“添加主机”按钮，如图 4-20 所示。然后在弹出的“DNS”对话框中，单击“确定”按钮。

图 4-20　“新建主机”对话框

（3）根据案例中的要求，建立相应的 E-mail、OA 的主机资源记录，最后单击“完成”按钮，如图 4-21 所示。

图 4-21　添加主机记录

（4）当所有的主机记录都添加完毕后，在正向查找区域 dhynet.com 中将出现相应的域名及 IP 的对应关系，如图 4-22 所示。

图 4-22　dhynet.com 区域的主机记录

（5）在企业的环境中，Web 服务器及 FTP 服务器共用一个 IP 地址 10.0.0.100，这种情况经常发生，当企业的服务承载量不大时，通常都会将多个服务集成在一台服务器上，为此需要建立相应的别名记录。右击区域 dhynet.com，在弹出的快捷菜单中选择“新建别名”，在弹出的“新建资源记录”对话框中输入“别名”为 ftp，通过单击“浏览”按钮在 dhynet.com 区域中找到 www，然后单击“确定”按钮，如图 4-23 所示。

图 4-23　“新建资源记录”对话框

（6）添加别名记录后，dhynet.com 区域中的记录如图 4-24 所示。

图 4-24　dhynet.com 区域中的资源记录

（7）打开客户端，单击“开始”→“运行”，在运行文本框中输入 cmd，单击“确定”按钮。在打开的命令行窗口中输入 nslookup 命令，在提示符下，输入域名进行验证，看 DNS 服务器是否能正确解析，如图 4-25 所示。

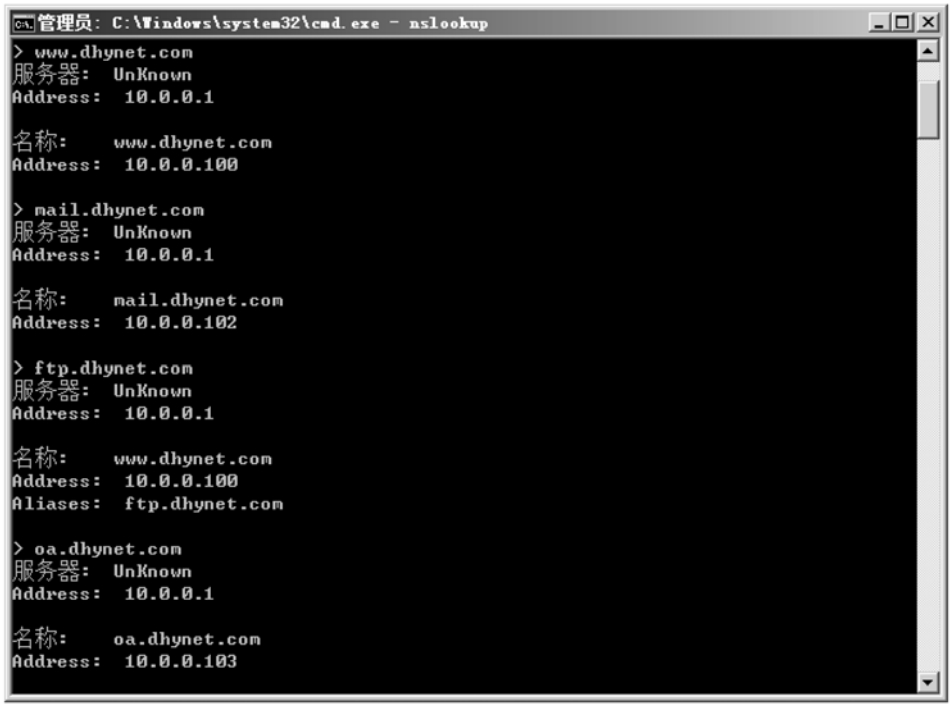

图 4-25　客户端进行域名解析测试

（8）在测试命令界面，我们发现“服务器：Unknown”，以及“Address：10.0.0.1”，这说明 DNS 服务器的名称没有被正确解析，同时在任务中要求根据 IP 地址能够解析出对应的 FQDN 名字，为了完成该任务，需要使用反向查找来完成。

右击“反向查找区域”，在弹出的快捷菜单中选择“新建区域”，如图 4-26 所示。

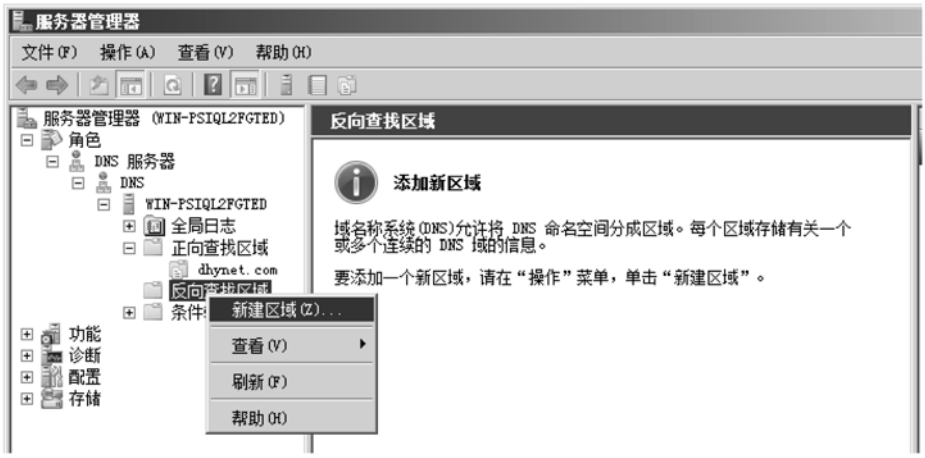

图 4-26　建立反向查找区域

（9）根据向导，选择新建主要区域，在反向查找区域名称步骤处选择“IPv4 反向查找区域”，在“反向查找区域名称”步骤中的“网络 ID”处填入公司服务器所用的 IP 地址的网络地址 10.0.0，单击“下一步”按钮，如图 4-27 所示。

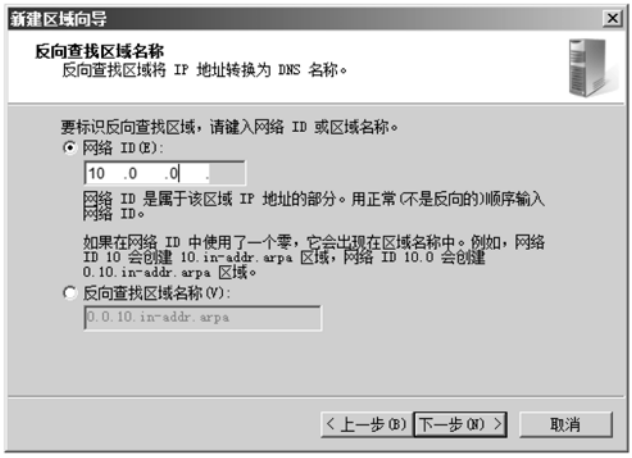

图 4-27　反向查找区域

（10）创建区域文件，并配置动态更新，检查摘要，确认无误后，单击“完成”按钮，如图 4-28 所示。

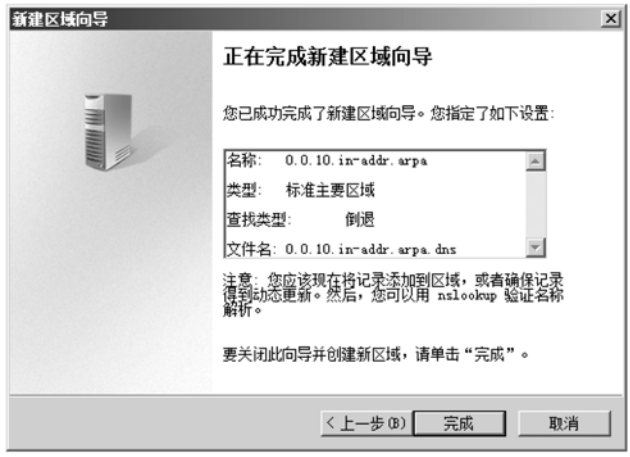

图 4-28　反向查找区域摘要信息

（11）建立完反向查找区域后，在“服务器管理器”控制台中的 DNS 角色中，将出现如图 4-29 所示的信息。

图 4-29　反向查找区域信息

（12）为了实现根据 IP 地址解析域名，需要在反向查找区域中为服务器建立指针记录。右击“反向查找区域”，在弹出的快捷菜单中选择“新建指针”选项，如图 4-30 所示。

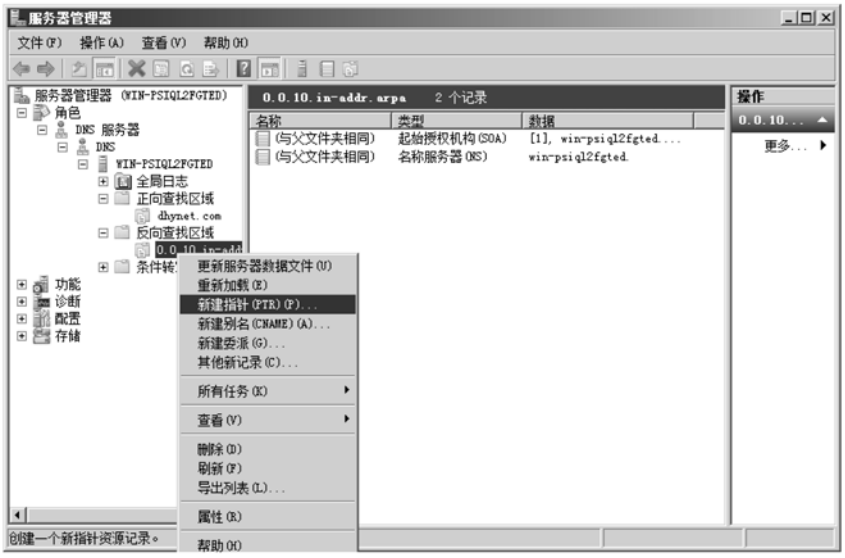

图 4-30　新建指针

（13）在“新建资源记录”对话框中的“主机 IP 地址”位置输入 Web 服务器的主机地址 10.0.0.100，然后通过单击“浏览”按钮，在 dhynet.com 域中找到对应的 FQDN 名，单击“确定”按钮，如图 4-31 所示。

图 4-31　建立指针记录

（14）使用同样的方法，将 OA、E-mail 等服务器的指针记录建立完毕，如图 4-32 所示。

图 4-32　在区域 10.0.0 中建立的指针记录

（15）通过客户端计算机运行 nslookup 命令，测试建立的反向指针记录，看是否能够进行正确的解析，如图 4-33 所示。

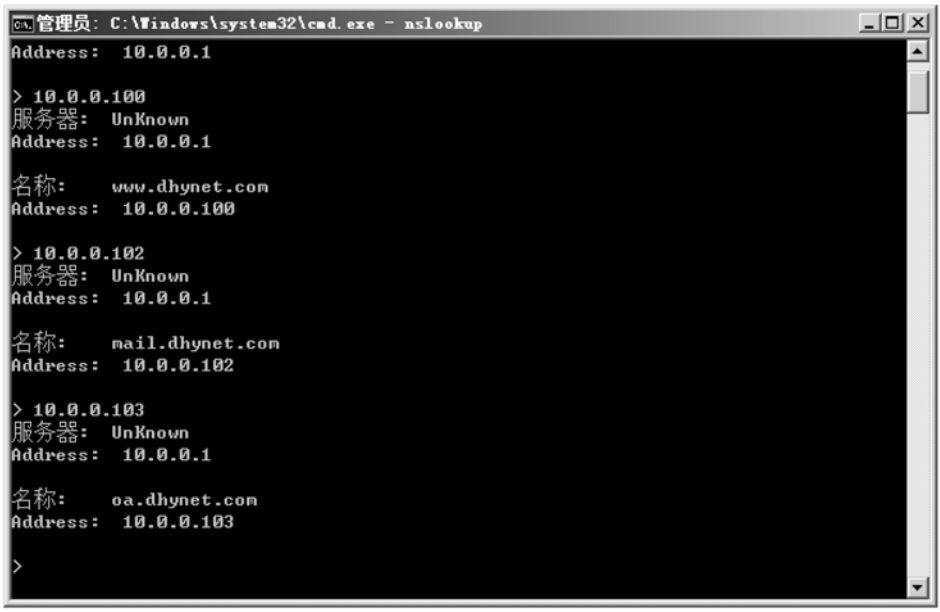

图 4-33　指针记录的测试

4.3.3　任务 3：邮件交换记录的建立及优先级的设置

1．案例分析

该公司每天都有大量的邮件需要处理，邮件服务也是公司最主要且最为繁重的业务，为了保证快速响应及可靠性，公司目前共设立了 2 台邮件服务器，名称分别为 win2k2.dhynet.com

和 win2k3.dhynet.com，对应的 IP 地址分别为 10.0.0.104 和 10.0.0.105，并且当 win2k2 无法联系时会自动切换到 win2k3 上工作。

当您将邮件发送到 SMTP 服务器时，邮件服务器必须将该邮件发送到目的地邮件服务器，也就是说邮件服务器要根据相应的收件箱的域名查找到目的地的邮件服务器地址，当然这也是 DNS 服务器的基本功能了，邮件服务器会向 DNS 服务器查找 MX 资源记录，因为 MX 记录负责记录某个域的邮件服务器。

2．实施过程

根据案例的要求，需要为该公司的邮件服务器建立相应的邮件交换记录，同时对存在的两台邮件服务器进行优先级的容错设置。

（1）先要保证在 dhynet.com 域中存在 win2k2 和 win2k3 的主机记录，然后再在 dhynet.com 域中建立 MX 记录。右击 dhynet.com 区域，在弹出的快捷菜单中选择“新建邮件交换器”，系统将弹出“新建资源记录”对话框。在该对话框中单击“浏览”按钮，在 dhynet.com 区域中找到 win2k2 的主机记录。邮件服务器优先级采用默认设置，如图 4-34 所示。

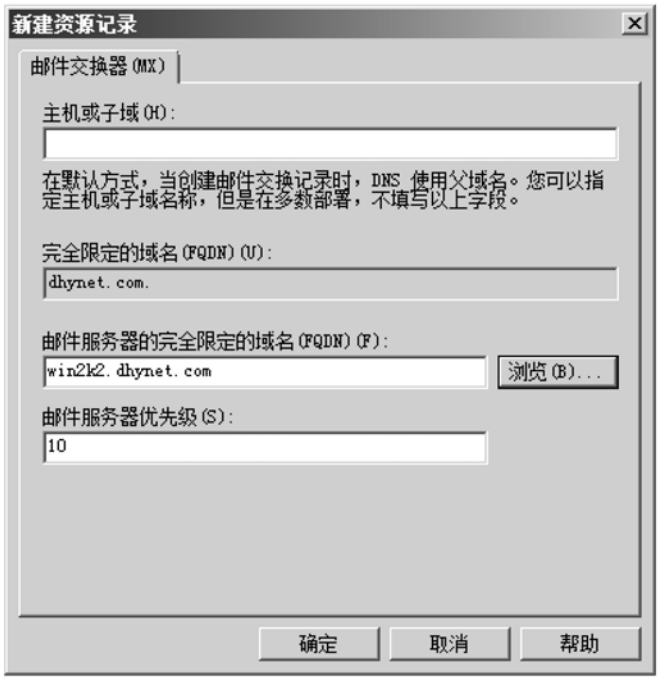

图 4-34　新建 MX 记录

（2）根据上步的内容完成 win2k3 主机的 MX 记录的添加，在优先级处确保 win2k3 的优先级数字大于 win2k2 的优先级数字，此处我们填写 30。在 DNS 中，MX 记录的优先级数字越大，则该服务器的优先级越低，数字越小，优先级越高，0 为最高优先级。通过设置优先级满足了当 win2k2 离线时，win2k3 能自动接替邮件服务器的工作，从而保证了该公司邮件服务的正常运行。配置好后的区域配置如图 4-35 所示。

图 4-35　建立不同优先级的 MX 记录

通过上述内容的设置，我们便完成了案例中的要求，同时也掌握了 DNS 服务器最基本及最常用的配置过程和配置方法。

4.4　知识能力拓展案例 2：创建 DNS 辅助区域

4.4.1　工作情景描述

DHYNET 公司在市场竞争中取得了较快的发展，吞并了 CISCONET 公司。为了保持原有的网络架构，该整合后的公司保留了两个公司原有的区域名称，分别是 dhynet.com 和 cisconet.com。为了保证该公司网络的高效及可利用性，每个区域放置了 1 台 DNS 服务器，同时为了保证总公司的可靠性，对 cisconet.com 域的 DNS 服务器建立了备份 DNS 服务器。

你需要完成如下工作。

（1）规划现有公司的 DNS 体系架构。

（2）dhynet.com 域中 DNS 服务器的 IP 地址是 10.0.0.1，cisconet.com 域中 DNS 服务器的 IP 地址是 10.0.0.222，备份 DNS 服务器的 IP 地址为 10.0.0.2。

（3）配置 dhynet.com 的区域，以便主机能够每 10 天更新一次各自的记录。

（4）配置 dhynet.com 域，以便没有经过 DNS 客户端更新的记录在 20 天后从 DNS 服务器上删除。

（5）清除备份 DNS 服务器上当前缓存的 DNS 名称解析。

（6）当 cisconet.com 域中的计算机访问 dhynet.com 域中的计算机时，最快速度的解析出 IP 地址。

4.4.2　案例分析

当采用备用 DNS 服务器时，需要使用辅助区域来建立辅助 DNS 服务器，并配置相应的区域传输。对主机更新的管理采用老化处理。

4.5　案例 2 实施过程

4.5.1　任务 1：建立辅助 DNS 服务器

（1）在备份 DNS 服务器上安装 DNS 服务，同时配置相应的 IP 地址及 DNS 服务器的 IP 地址，如图 4-36 所示。

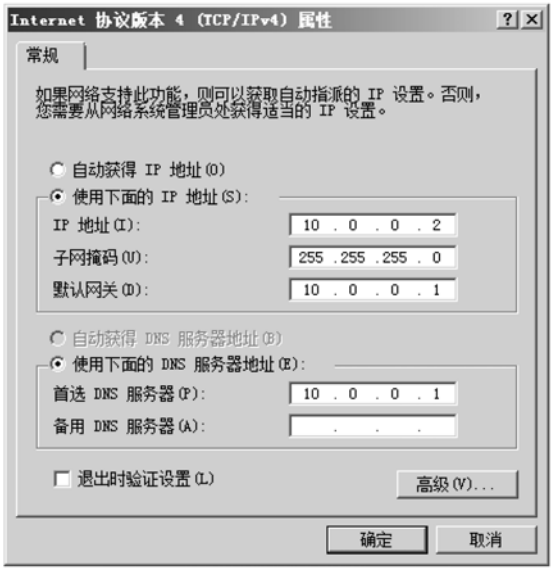

图 4-36　辅助 DNS 服务器的 TCP/IP 属性设置

（2）在备份 DNS 服务器上打开服务器管理控制台，选择 DNS 角色，创建区域，在“新建区域向导”对话框的“区域类型”步骤中的“选择您要创建的区域的类型”中选择“辅助区域”，如图 4-37 所示。

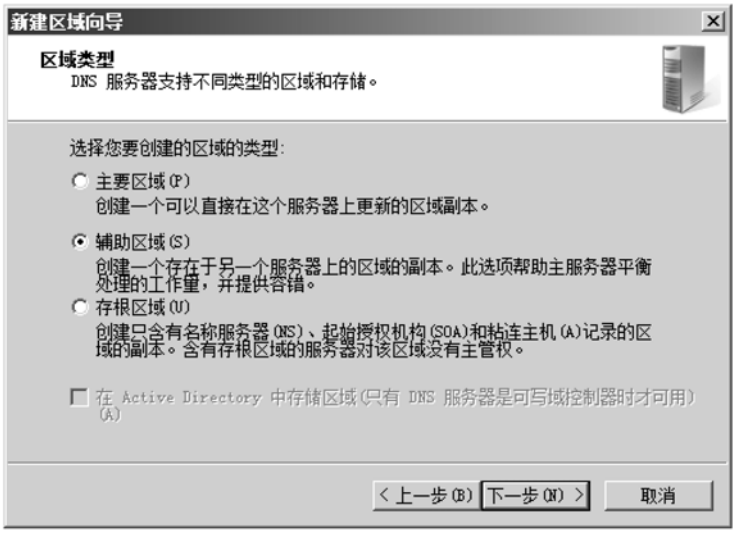

图 4-37　“辅助区域”的建立

（3）在“区域名称”中填入要复制的主要区域的 DNS 区域名称，此处为 dhynet.com，如图 4-38 所示。

图 4-38　设置要复制的区域名称

（4）在主 DNS 服务器处，单击提示区域并填写要复制区域的主 DNS 服务器的 IP 地址，此处为 10.0.0.1。设置完成后，单击“下一步”按钮，如图 4-39 所示。在“新建区域向导”对话框的“正在完成新区域向导”步骤中，查看摘要，确认无误后，单击“完成”按钮。

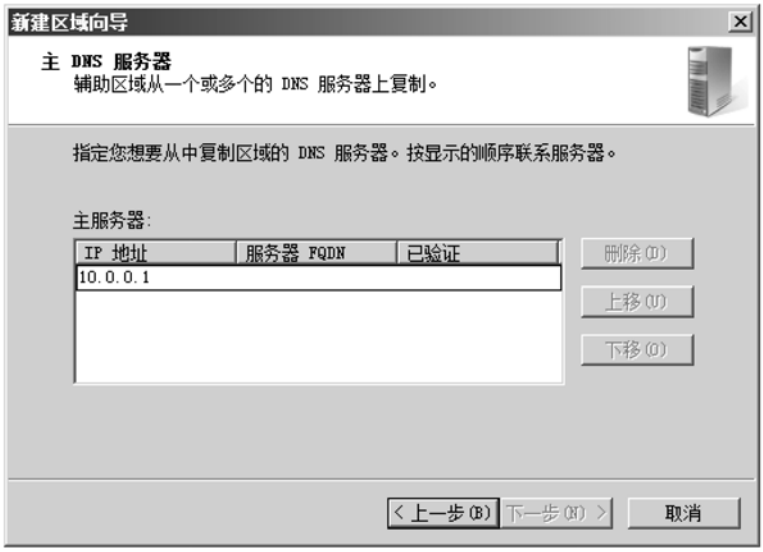

图 4-39　设置主 DNS 服务器的 IP 地址

（5）辅助 DNS 服务器设置完成后，还不能马上完成复制的实现，必须在相应的主 DNS 服务器上进行相应的设置。在主 DNS 服务器上打开 DNS 管理控制台，确保有辅助 DNS 服务器的主机记录。如果辅助 DNS 服务器没有动态注册进来，可以采用手动添加一条静态记录的方法，如图 4-40 所示。

图 4-40　主 DNS 服务器的区域中应该有辅助 DNS 服务器的主机记录

（6）配置了资源记录后，必须要做的是启用主 DNS 服务器的区域复制功能。在 dhynet.com 区域中右击选择“属性”，在打开的“属性”对话框中，选择“区域传送”选项卡，确保“允许区域传送”选项被选中，并勾选“只允许到下列服务器”单选按钮，如图 4-41 所示。然后单击“编辑”按钮，在“允许区域传送”对话框中，单击提示区域并添加许可传送的备用 DNS 服务器的 IP 地址，此处是 10.0.0.2。

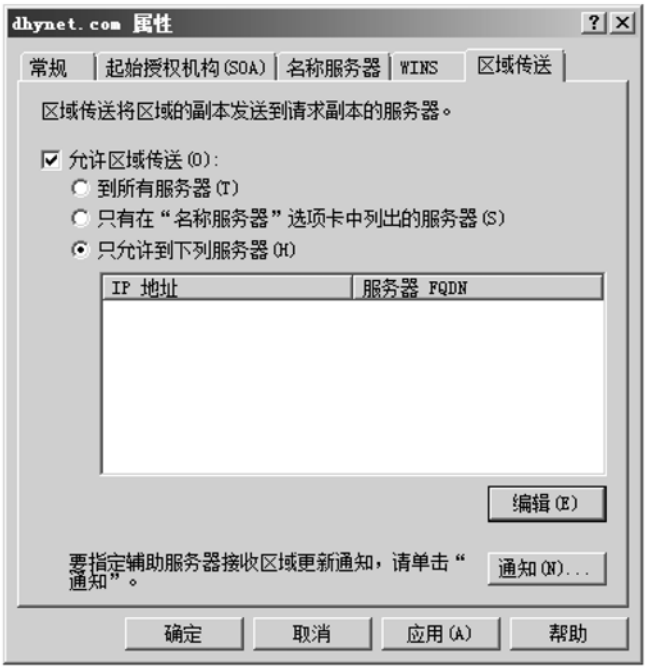

图 4-41　“区域传送”选项卡的设置

（7）设置完成后，将显示如图 4-42 所示的内容。

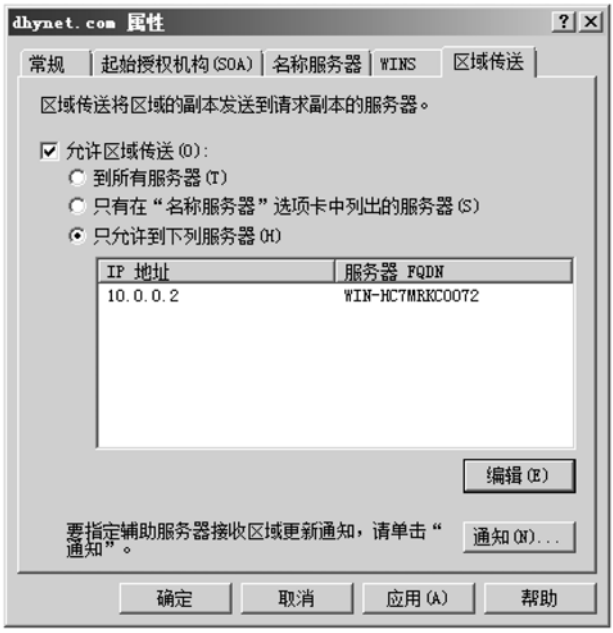

图 4-42　名称服务器的设置

（8）在辅助 DNS 服务器的 dhynet.com 区域上右击选择“从主服务器复制”，完成辅助 DNS 服务器的数据复制过程。

4.5.2　任务 2：老化和清理的设置

要完成主机记录的更新，需要配置 DNS 服务器的老化和清理选项。

（1）在 dhynet.com 域的 DNS 服务器上右击选择“为所有区域设置老化/清理”，如图 4-43 所示。

图 4-43　选择“为所有区域设置老化/清理”

（2）在“服务器老化/清理属性”对话框中，按照要求将“无刷新间隔”和“刷新间隔”均设置为 10 天，同时选中“清除过时资源记录”，如图 4-44 所示。

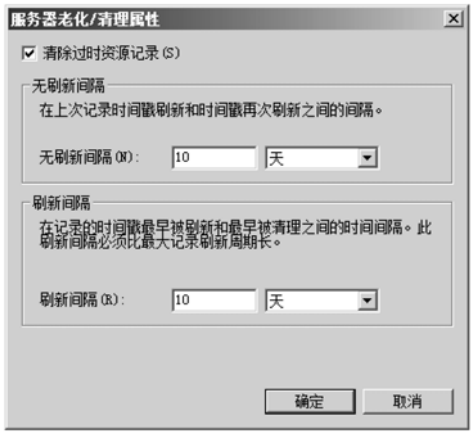

图 4-44　设置刷新时间

（3）为了马上清除缓存资源，可以在服务器上右击选择“清除缓存”，如图 4-45 所示。

图 4-45　“清除缓存”命令

（4）为了能够马上对 cisconet.com 域中的客户端提供 dhynet.com 域的 FQDN 的解析，可以使用 DNS 服务器的转发器功能。在 dhynet.com 区域右击选择“属性”，然后在“属性”对话框中选择“转发器”选项卡，单击“编辑”按钮，再单击提示区域输入要转发的 DNS 服务器地址，此处添加 10.0.0.2。其他选项保持默认设置，设置完成后，单击“确定”按钮，如图 4-46 所示。

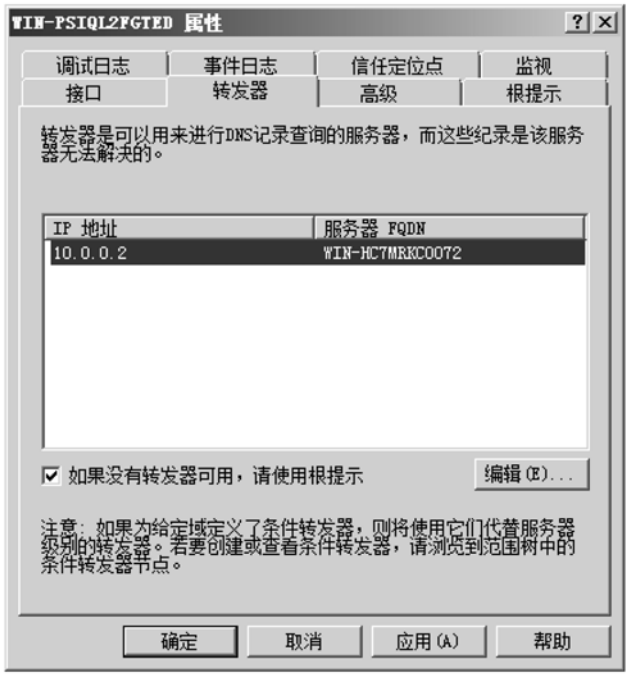

图 4-46　“转发器”选项卡

4.6　项目完成结论

通过完成本项目，学习了如何安装 DNS 服务角色，如何配置及管理 DNS 服务，对 DNS 服务中的区域创建、记录创建、记录查询进行了系统的实例应用练习。当然，DNS 服务角色的应用还有很多，但是限于篇幅，本章不再列举其他应用，其他诸如区域委派、权限委派等知识点请读者自行到微软官方网站参考学习。

4.7　练 习 案 例

你是公司的网络管理员。公司名为 FABRIKAM。公司网络由名为 fabrikam.com 的单一 Active Directory 域组成。

你在数据中心一台新的 Windows Server 2008 计算机上安装了 DNS。你将该计算机命名为 server1，并配置其 IP 地址为 10.10.30.54。你在 server1 上安装了两个网卡，并将 server1 配置成一台域控制器。server1 有两个网卡，一个具有公用 IP 地址，另一个具有专用 IP 地址。专用子网是 10.10.30.x。

研发部使用一个名为 test.local 的域，该域存储在一台独立的 UNIX DNS 服务器上。此服务器被配置的 IP 地址为 10.10.50.100。

FABRIKAM 与名为 CONTOSO 的公司合并。CONTOSO 公司的网络由名为 contoso.com 的单一 Active Directory 域组成。两个域仍然保持独立。

你必须在 server1 上配置 DNS，以确保能满足下列要求。

（1）来自客户端计算机对 contoso.com 上主机的名称解析请求，如被指派查询 server1，则必须由 contoso.com 域中 IP 地址为 10.150.10.100 的 DNS 服务器直接解析。

（2）server1 上必须有一份 test.local 的安全副本。

（3）必须为 10.10.30.x 子网创建反向查找区域。该区域必须存储在 Active Directory 域中，所有更新都应是安全的。

（4）DNS 服务器应仅响应来自专用网络的请求。

4.8 课 后 习 题

1．DNS 有哪两种查询方式？

2．什么是 DNS？

3．DNS 服务角色可以注册哪些记录类型，分别有什么样的作用？

4．列举主要的 DNS 顶级域名并说出其中文名称。

5．简述区域复制的作用和目的。

6．简述客户端向本地网络中 DNS 服务器发出查询 www.dhynet.com 主机 IP 地址的详细过程。

7．简述如何设置 DNS 区域复制。

项目 5　应用程序服务的安装、配置与管理

在企业网和因特网中，应用服务器是被广泛使用的，常用的有 Web 服务器和 FTP 服务器。Web 服务器提供企业网站的对外网站服务和内部网站服务，FTP 服务器提供了文件资料的上传和下载功能，这在企业中都是常用业务。通过本章的学习，将能够掌握如下的知识技能点，在实际使用中可以根据需要架设 Web 站点，并开通 FTP 服务。

知识点、技能点

- 安装 Web 服务器和 FTP 服务器
- 配置 Web 服务器提供网站服务
- 掌握虚拟站点的配置
- 配置 FTP 服务器，提供文件上传下载服务
- 不同身份的 FTP 用户具有不同权限

5.1　引例：为什么要使用应用服务器（WHY）

现代企业都需要宣传自己，而因特网是一个最好的宣传平台，企业只要在网络上发布自己的网站，就可以让全世界的人来看，从而达到自我宣传的目的。在企业内部，往往也需要有内部网站，以便进行企业内部信息发布、交流，这都需要用到应用服务器中的 Web 服务器。另外，在网络上，还常常会有文件资料、视频资料的上传和下载，FTP 服务器就是最简单有效的文件上传、下载服务器，可以完全满足这些需求。

1．什么是 Web 服务器

Web 服务器也称为 WWW（World Wide Web）服务器，主要功能是提供网上信息浏览服务。它在应用层使用 HTTP 协议，对 HTML 文档格式提供支持，通过浏览器统一资源定位器（URL）进行访问。

WWW 是 Internet 的多媒体信息查询工具，是 Internet 上近年才发展起来的服务，也是发展最快和目前应用最广泛的服务。正是因为有了 WWW 工具，才使得近年来 Internet 迅速发展，且用户数量飞速增长。

2．什么是 FTP 服务器

FTP 服务器是在因特网上提供存储空间的计算机，它们依照 FTP 协议提供服务。FTP 的全称是 File Transfer Protocol（文件传输协议）。顾名思义，就是专门用来传输文件的协议。简单地说，支持 FTP 协议的服务器就是 FTP 服务器。

一般来说，用户上网的首要目的就是实现信息共享，文件传输是信息共享非常重要的一个内容之一。Internet 上早期实现传输文件，并不是一件容易的事，我们知道 Internet 具有一个非常复杂的计算机环境，有 PC、有工作站、有 MAC、有大型机，据统计连接在 Internet 上的计算机已有上千万台，而这些计算机可能运行不同的操作系统，有运行 UNIX 的服务器，也有运行 DOS、Windows 的 PC，还有运行 MacOS 的苹果机，等等，而各种操作系统之间的文件交流，需要建立一个统一的文件传输协议，这就是 FTP。基于不同的操作系统有不同的 FTP 应用程序，而所有这些应用程序都遵守同一种协议，这样用户就可以把自己的文件传送给别人，或

者从其他的用户环境中获得文件了。

5.2　案例 1：构建 Web 服务

5.2.1　工作情景描述

DHYNET 公司内部网络已经正常使用了，现为了提高信息传达效率，让员工能够及时了解和掌握公司的信息，需要在公司内部架设 Web 网站，用于发布内部信息。在开始的网络规划时，已经把 192.168.2.66 专门留给了 Web 服务器，供其使用。网络管理员现需要配置一台 Windows Server 2008 的服务器，将其配置为 Web 服务器，使用该 IP 地址，为公司内部提供 Web 网站服务。

5.2.2　案例分析

在本项目中，Windows Server 2008 的服务器已经存在，我们需要在其上安装并配置好 Web 程序，以使其能够对内提供网站服务。实现的思路如下：

- 安装 Web 服务器程序；
- 配置 Web 服务器提供网站服务；
- 测试 Web 服务器运行。

5.2.3　相关知识

Web 服务器工作原理，如图 5-1 所示。

- Web 服务器与客户机通过网络连接在一起。
- Web 服务器上具有可以被访问的网站。
- 客户机可通过浏览器发起 Web 浏览请求。

图 5-1　Web 服务器工作原理

5.3　案例 1 实施过程

5.3.1　任务 1：Web 服务器角色的安装

1．案例分析

为了能够提供 Web 服务，让客户机能够访问 Web 内容，作为管理员，你需要在网络中安

装 Web 服务器。在 Windows Server 2008 系统中没有默认安装 Web 服务，因此需要安装 Web 服务。安装 Web 服务的机器要使用固定 IP（本例中使用 192.168.2.66）。

2．实施过程

（1）单击“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口，单击“角色”，如图 5-2 所示。

图 5-2　“服务器管理器”窗口

（2）单击“添加角色”，然后单击“服务器角色”，即可对所要添加的角色进行选择，勾选“Web 服务器（IIS）”，如图 5-3 所示，此时弹出如图 5-4 所示的对话框，单击“添加必需的功能”按钮，然后单击“下一步”按钮。

图 5-3　勾选“Web 服务器（IIS）”角色

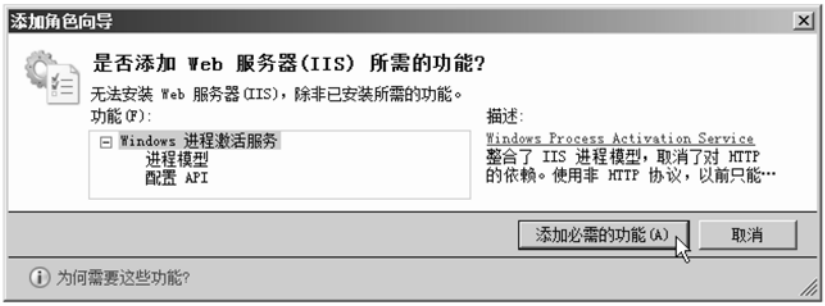

图 5-4　单击“添加必需的功能”按钮

（3）在出现的 IIS 服务器介绍对话框中单击“下一步”按钮，进入“角色服务”对话框，根据需要选择所需的角色服务，如勾选 ASP.NET，则会自动勾选.NET 扩展性、ISAPI 扩展和 ISAPI 筛选器项。

（4）单击“下一步”按钮，确认所选内容后，单击“安装”按钮，完成后单击“关闭”按钮。

安装完成后，运行 IE 浏览器，在地址栏输入 127.0.0.1，访问本机，出现如图 5-5 所示的界面，即表示 IIS 工作正常了。我们还可以在同一网段的其他机器上通过浏览器访问 192.168.2.66，即 Web 服务器的 IP 地址，如果也出现如图 5-5 所示的内容，则表示 Web 服务器可以在网络中提供正常服务了。

图 5-5　测试页面

5.3.2　任务 2：配置 IIS 服务器，提供网站服务

1．案例分析

现在，我们已经有一个可以正常运行的 Web 服务器了，但它现在还没有网站可供其他人浏览。我们需要对其进行一些设定，以保证可以让其他人访问。

2．实施过程

（1）单击“开始”→“管理工具”→“Internet 信息服务（IIS）管理器”，进入“Internet

信息服务（IIS）管理器”界面。单击“网站”前的“+”号，出现“Default Web Site”，单击该项目，将会出现该站点的“功能视图”，如图 5-6 所示。

图 5-6　默认站点选项内容

（2）单击右侧“操作”框下的“浏览”按钮，即可打开默认网站所对应的文件夹，位置是“C:\inetpub\wwwroot”，在这里存放着默认网站文件，如图 5-7 所示（其中 iisstart.html 和 welcome.png 是默认的测试页面和图片）。我们可以把网站内容放到该目录下，即可被访问。

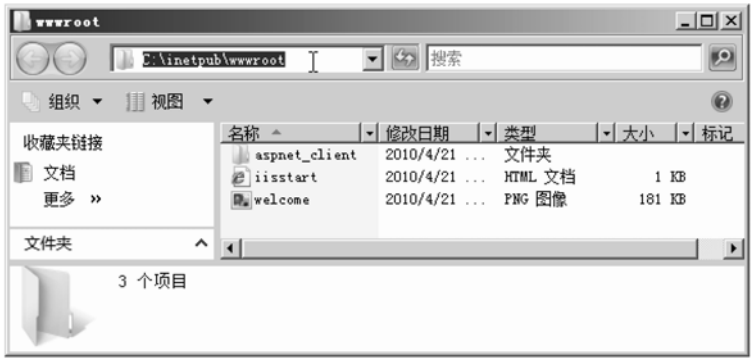

图 5-7　Web 默认文档内容

（3）创建一个.html 文件，测试访问情况，如图 5-8 所示。

图 5-8　自定义页面内容

可以通过 DNS 系统，建立起 oa.dhynet.com 与 192.168.2.66 的解析记录，从而使用域名访问 OA 系统。如没有建立 DNS 记录，则只能使用 IP 地址进行访问。

5.4　案例 2：建立新网站

5.4.1　工作情景描述

公司现在已经可以正常使用 OA 系统进行网络办公了，随着公司业务的发展，现公司还需要建立多个部门的网站，公司希望在最小开销的情况下完成这个需求。也就是说，尽量使用当前已有的资源完成多个部门网站的建立。

5.4.2　案例分析

在最小开销的情况下完成此需求，即利用当前的 Web 服务器完成此需求。在这里，我们可以使用 Web 服务器的两个功能，即虚拟目录和新建站点，均可以完成这个需求。

5.4.3　相关知识

虚拟目录和新建站点方式的区别如下。

使用虚拟目录时，访问方式为“http://dhynet.com/名称”，如“http://dhynet.com/oa”，这种方式把 OA 站点作为 dhynet.com 下的一个目录来进行访问，这个方法实现起来最简单、方便，不需要另外进行 DNS 解析记录的建立。

使用新建站点时，访问方式为“http://名称.dhynet.com”，如“http://oa.dhynet.com”，这种方法将 OA 站点作为一个独立的网站进行访问，需要有单独的 IP 地址与之对应，访问方式符合 FQDN 名称方式，但需要另外进行“一卡对多 IP”的设置和 DNS 解析记录的建立，才能正常访问。

5.5　案例 2 实施过程

5.5.1　任务 1：使用虚拟目录建立网站

1．案例分析

要使用虚拟目录方式来建立其他部门的 Web 站点，我们需要先建立这个部门的网站目录，然后使用 Web 服务器自身的新建虚拟目录功能，将其指定到该目录上，即可完成。

2．实施过程

（1）在“Internet 信息服务（IIS）管理器”中，右击“Default Web Site”，选择“添加虚拟目录”，如图 5-9 所示。

图 5-9　添加虚拟目录

（2）在“添加虚拟目录”对话框中，输入“别名”（此处假设为 sales），并单击“物理路径”后的按钮，指定 sales 的网站文件路径，如图 5-10 所示，然后单击“确定”按钮。

图 5-10　设置虚拟目录属性

完成后，IIS 管理器界面中的“Default Web Site”下，将会出现“salse”虚拟目录项，如图 5-11 所示。

图 5-11　建立好的虚拟目录

此时，即可使用“http://dhynet.com/salse（已建立 dhynet.com 的 DNS 记录）”访问了，如图 5-12 所示。

图 5-12　虚拟目录访问（域名访问方式）

或者使用“http://192.168.2.66/salse（未建立 dhynet.com 的 DNS 记录）”来进行访问，如图 5-13 所示。

图 5-13　虚拟目录访问（IP 访问方式）

5.5.2　任务 2：使用新建站点建立网站

1．案例分析

使用新建站点的方式建立网站，要比虚拟目录方式复杂，但从访问形式上更规范。首先要对网卡进行“一卡对多 IP”的设定，其次要有部门的网站目录及相应的网站文件，然后使用 Web 服务器的“新建站点”功能进行设置，最后再建立起相应域名的 DNS 主机记录，才可正常访问建立好的网站。

2．实施过程

（1）设置“一卡对多 IP”。在网卡的“TCP/IP 属性”对话框中，单击“高级”按钮。在打开的“高级 TCP/IP 设置”对话框的“IP 设置”选项卡的“IP 地址”选项组中单击“添加”按钮，输入新建网站所使用的 IP 地址（假设为 192.168.2.100），设置完成后的效果如图 5-14 所示。单击“确定”按钮，完成设置。

图 5-14　设置多 IP 地址

（2）在“Internet 信息服务（IIS）管理器”对话框中，右击“网站”，选择“添加网站”，如图 5-15 所示。

图 5-15　添加网站

（3）在“添加网站”对话框中，进行相应的设置，如图 5-16 所示，单击“确定”按钮完成设置。

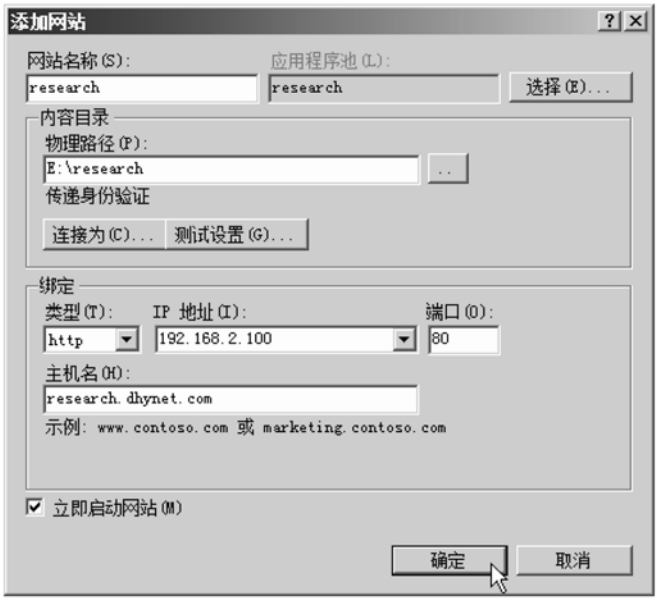

图 5-16　设置网站属性

（4）完成后，IIS 管理器界面中，将会出现“research”网站，如图 5-17 所示。

图 5-17　建立好的网站

（5）在 DNS 服务器上，建立 research.dhynet.com 的主机记录，对应 IP 地址为 192.168.2.100（此部分请参阅相关章节资料）。

（6）使用 http://research.dhynet.com 访问，即可访问到研发部的站点了，如图 5-18 所示。

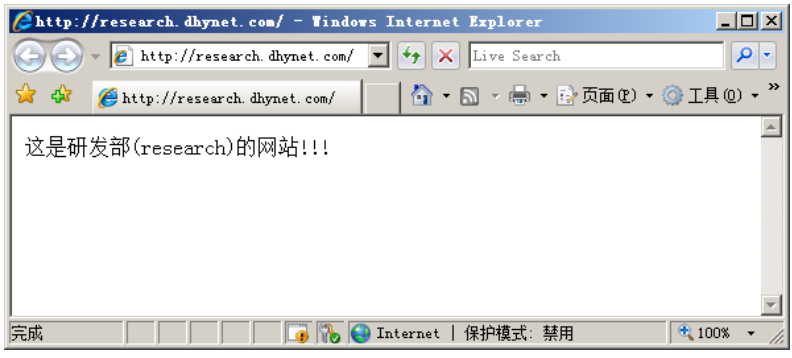

图 5-18　访问 research 网站

在实际使用中，可以视具体情况，来确定使用哪种方式实现一台服务器提供多网站服务的功能。

本项目提出的需求，经过分析后，需要达到以下目的：

- 安装 Web 服务器功能。
- 配置 Web 服务器，提供内部 OA 网站服务。
- 在最小化资源的前提下，为公司其他部门提供网站服务。

为了完成任务，我们在 Windows Server 2008 上安装了 Web 服务器角色功能，并对其进行了基本配置，以满足 OA 网站的浏览功能。随后，我们又使用了两种方法（虚拟目录和新建网站）完成了对公司其他部门提供网站服务的需求。

5.6　案例 3：建立 FTP 服务

5.6.1　工作情景描述

公司的销售部（sales）和研发部（research）需要在公司内部进行一些文件的交换与保存，他们希望这些操作尽可能的方便，不需要使用 U 盘等外部存储设备就能进行文件的保存与交换。

5.6.2　案例分析

为了满足销售部（sales）和研发部（research）的文件保存和交换的需求，可以使用 FTP 服务器来完成这个任务。给普通员工（sales users 和 research users）有上传文件和下载文件的权限，且只能上传文件到本部门所属的文件夹下，而完全权限（包括删除权限）则给部门经理（sales manager 和 research manager），从而达到安全使用的目的。

5.6.3　相关知识

FTP 权限与 NTFS 权限。

在 FTP 文件的上传/下载中，涉及到了文件操作权限的设定，而要达到安全控制，只使用 FTP 服务器本身的文件权限控制是不够的，必须使用 NTFS 权限和 FTP 权限相结合的方式来进行控制。

当 FTP 权限和 NTFS 权限叠加时，最终权限效果将是二者的交集，如表 5-1 所示。

表 5-1　权限设定要求

权限类型 / 用户	FTP 权限	NTFS 权限	最终权限
A	下载（读），写（上传），删除	读	下载（读）
B	下载（读），写（上传），删除	读，写	下载（读），写（上传）
C	下载（读），写（上传），删除	读，删除	下载（读），删除

注意：关于 NTFS 权限请参阅相关章节及资料。

5.7　案例 3 实施过程

5.7.1　任务 1：FTP 服务器角色的安装

1．案例分析

要使用 FTP 功能，首先必须安装 FTP 服务器。

2．实施过程

（1）单击“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口。展开“角色”前的“+”号，在出现的“Web 服务器（IIS）”上单击鼠标右键，在弹出的菜单中选择“添加角色服务”，如图 5-19 所示。

图 5-19　添加角色服务

（2）在出现的“添加角色向导”对话框的“选择服务器角色”步骤中，勾选最下面的“FTP 发布服务”，此时会出现“添加必需的角色服务”确认框，确认后，如图 5-20 所示。

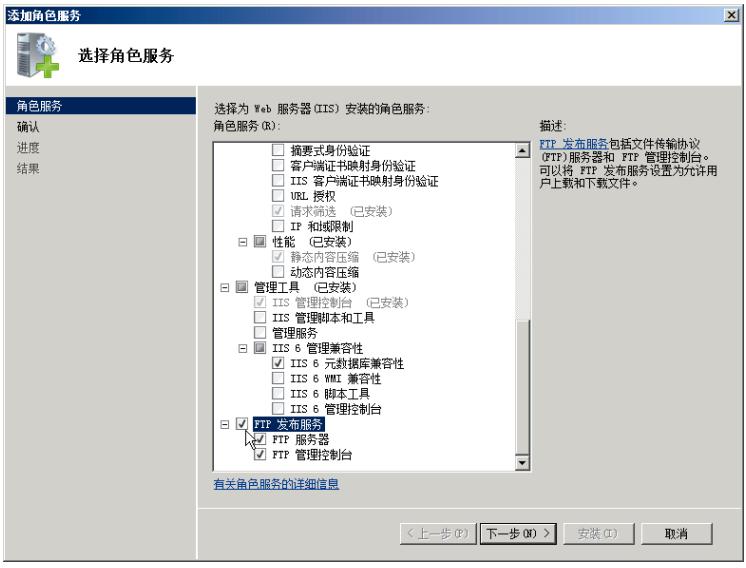

图 5-20　勾选 Web 服务器

（3）单击“下一步”按钮，然后单击“安装”按钮。

（4）完成安装后，在“管理工具”下会出现“Internet 信息服务（IIS）6.0 管理器”项，单击此项即可进入 FTP 站点管理窗口。依次展开各“+”号，最终会看到默认 FTP 站点“Default FTP Site”，此时 FTP 功能还没有运行，右击“Default FTP Site”，选“启动”，最终情况如图 5-21 所示。

图 5-21　默认 FTP 站点

（5）现在可以在资源管理器的地址栏中，使用 ftp://192.168.2.88（未建立 DNS 记录）或 ftp://ftp.dhynet.com（已建立 DNS 记录）来访问 FTP 站点了，如图 5-22 所示。

图 5-22　访问 FTP 站点

注意：此时的默认 FTP 站点目录是 C:\inetpub\ftproot，没有任何文件，因此显示的内容是空的。

5.7.2　任务 2：设置 FTP 服务器，满足项目任务需求

1．案例分析

在这个项目中，对于不同身份的用户，需要有不同的 FTP 访问权限，权限需求如表 5-2 所示。

表 5-2　各用户访问权限需求

身　份	文 件 夹	访问权限需求
Sales users	sales	写（上传），下载（读）
Sales manager		写（上传），下载（读），删除
Research users	research	写（上传），下载（读）
Research manager		写（上传），下载（读），删除

除以上权限外，sales 部门的用户和经理无权对 research 部门的文件夹进行下载（读）操作以外的任何操作。

根据以上总结的权限，我们可以最终确认以下的 FTP 与 NTFS 的权限设定需求（请注意：对于一个 FTP 站点来说，要保证用户可以写入文件，必须开启整个 FTP 站点的写入权限，而对具体目录的写操作限制，则由 NTFS 权限来进行限制，最终权限是 FTP 权限与 NTFS 权限的交集）。

（1）sales 部门员工对 sales 文件夹和 research 文件夹的权限，如表 5-3 所示。

表 5-3　sales 部门员工访问权限

身　份	文 件 夹	FTP 权限	NTFS 权限
Sales users	sales	上传（写），下载（读）	读，写（包括创建目录）
Sales manager		上传（写），下载（读）	读，写（包括创建目录），删除
Sales users	research	下载（读）	读
Sales manager		下载（读）	读

（2）research 部门员工对 sales 文件夹和 research 文件夹的权限，如表 5-4 所示。

表 5-4　research 部门员工访问权限

身　份	文 件 夹	FTP 权限	NTFS 权限
research users	sales	下载	读
research manager		下载	读
research users	research	上传，下载	读，写（包括创建目录）
Research manager		上传，下载，删除	读，写（包括创建目录），删除

2．实施过程

（1）创建用户及组，以便设置访问权限，相关信息如表 5-5 所示（用户和组的添加请参考相关资料）。

表 5-5　创建组及用户相关信息

组	组　员	密　码
sales users	tom	tom99!@#
	john	john!@#$
sales manager	ben	benp@sswd
research users	lqy	p@sswd99

续表

组	组　员	密　码
research manager	dim	p@sswd77
	jim	jim!@#66

（2）单击“开始”→“管理工具”→“Internet 信息服务（IIS）6.0 管理器”，展开 FTP 站点，右击“Default FTP Site”，选择“属性”，在打开的“属性”对话框的“FTP 站点”标签下，进行如图 5-23 所示的设置。

图 5-23　“FTP 站点”标签

（3）单击“安全帐（账）户”标签，取消“允许匿名连接”的勾选，也就是必须使用用户名和密码进行访问，如图 5-24 所示。当然，也可以允许使用匿名连接，具体看使用情况而定。在本例中，为了安全，我们必须使用用户名和密码访问。

图 5-24　设置 FTP 站点安全账户

（4）单击“主目录”标签，进行如图 5-25 所示的设置。

注意：在“FTP sit”目录下，我们已经创建了 sales 文件夹和 research 文件夹。

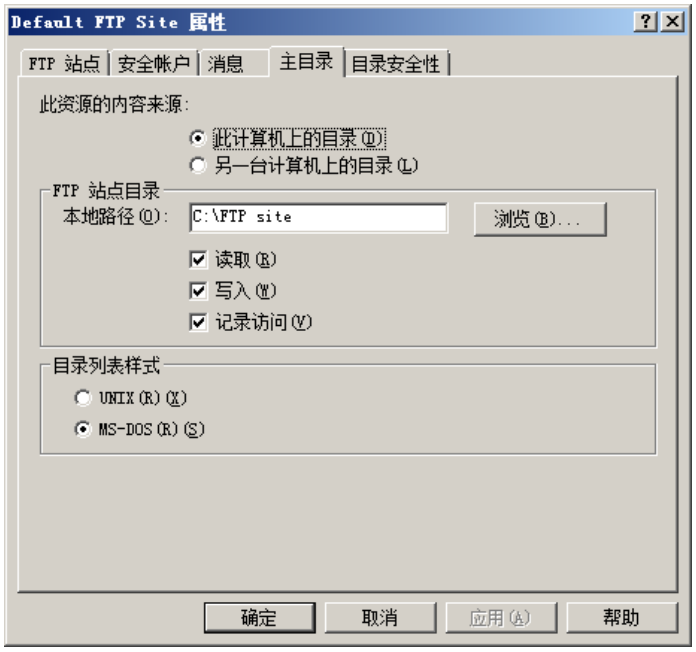

图 5-25　设置 FTP 站点目录

此时，我们已经可以使用 ftp://192.168.2.88（未建立 DNS 记录）或 ftp://ftp.dhynet.com（已建立 DNS 记录）来访问设置好的 FTP 站点了（此时的目录已经不是默认的位置了，已经更改为我们设定的“FTP site”目录了），如图 5-26 所示。

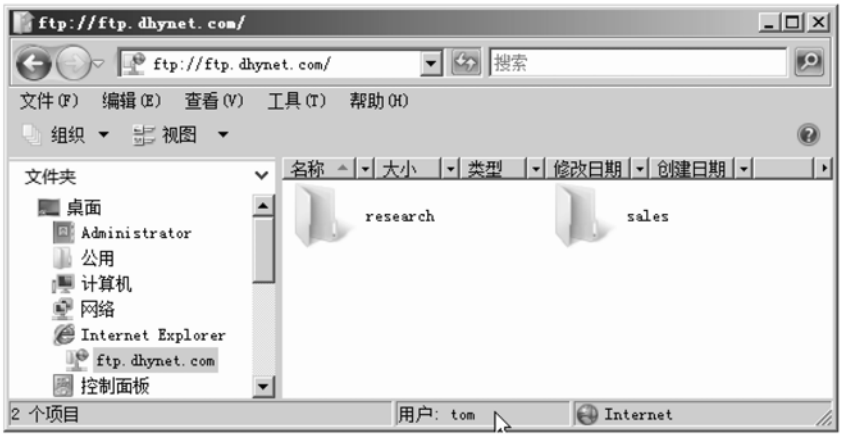

图 5-26　访问 FTP 站点

（5）此时，我们可以正常访问两个部门的 FTP 文件夹了，但相关权限并不完整，现在需要对文件夹的 NTFS 权限进行设定，最终达到案例分析中所要求的权限。各文件夹权限的设定如表 5-6 到表 5-8 所示（关于 NTFS 权限设定的方法，请参阅相关章节资料，此处不再详述）。

表 5-6　不同用户组对站点根目录的访问权限

文　件　夹	身　　份	NTFS 权限	继　承　性
ftp site	sales users	读取和执行 列出文件夹目录 读取	不向下继承
	sales manager		
	research users		
	research manager		

表 5-7　不同用户组对 sales 文件夹的访问权限

文　件　夹	身　　份	NTFS 权限	继　承　性
sales	sales users	读取和执行 列出文件夹目录 读取 写入	不继承父文件夹权限
	sales manager	完全控制	
	research users	读取和执行 列出文件夹目录 读取	
	research manager	读取和执行 列出文件夹目录 读取	

表 5-8　不同用户组对 research 文件夹的访问权限

文　件　夹	身　　份	NTFS 权限	继　承　性
research	sales users	读取和执行 列出文件夹目录 读取	不继承父文件夹权限
	sales manager	读取和执行 列出文件夹目录 读取	
	research users	读取和执行 列出文件夹目录 读取 写入	
	research manager	完全控制	

经过以上设定后，FTP 服务器即可正常运行，并能达到案例分析中所设定的需求了。使用不同身份的用户登录 FTP，进行各种读/写操作进行验证即可。

在本案例中，主要是使用 FTP 服务器来完成公司内部文件的保存和交换，同时各部门的用户对其他部门的文件夹只能读取，不能进行写操作和修改操作。

要完成这个目的，我们完成的内容有以下几项。

- 安装 FTP 服务器。
- 建立所需文件夹，并设置 FTP 服务器能够访问的文件夹。
- 创建访问 FTP 服务器的用户组和用户。
- 设置 FTP 服务器的访问权限和不同用户（组）对 FTP 文件夹的 NTFS 访问权限，在两个权限相互作用的交集下，产生项目需求的最终权限。

以上，是完成此案例思路的总结。至此，我们已经完成了本案例的需求。

5.8　项目完成结论

在本项目的案例中，学习了安装 Web 服务器和 FTP 服务器的方法。

在 Web 服务器配置中，学习了基本的网站配置方法，并在此基础上，进行了高级配置。根据需求的访问形式不同，采用虚拟目录或虚拟站点的方式，对 Web 服务器进行了不同的配置，以达到最好的访问效果。

在 FTP 服务器配置中，针对不同身份用户的不同访问需求，配置 FTP 服务器的不同访问权限。针对组用户访问，创建了组及组中的用户，并将 FTP 访问权限和 NTFS 文件系统访问权限相结合，灵活控制用户的访问权限，做到既安全又高效。

5.9　练习案例

公司现因发展需要，计划建立名为 news.dhynet.com 的新闻站点，并利用 FTP 功能对这个站点的所有文件进行维护操作，站点维护员是 Tina，你需要如何设定？

5.10　课后习题

1．作为公司的网络管理员，你在网络中的一台名为 FTPServer 的 Windows Server 2008 计算机上创建了一个 FTP 站点，允许用户对站点的内容进行下载的操作，站点的主目录位于 NTFS 分区，并设置这个站点不允许匿名访问。这台 FTP 服务器上有两个用户账号 User1 和 User2，其中 User1 是 administrators 组的成员，User2 是普通账号。当使用账号 User1 访问 FTP 服务器时没有任何问题，可是当使用账号 User2 访问 FTP 服务器时，系统提示登录失败。你应该采取什么措施解决这个问题？（　　）

A．设置 FTP 站点允许匿名访问

B．把用户账号 User2 加入 administrators 组

C．在主目录文件夹的 NTFS 访问权限中赋予用户 User2“读取”权限

D．在 FTP 服务器上把用户账号 IUSR_FTPServer 激活

2．你在一台 Windows Server 2008 计算机上实现了 FTP 服务，在一个 NTFS 分区上创建了主目录，允许用户进行下载，并允许匿名访问。可是 FTP 的用户报告说他们不能下载服务器上的文件，通过检查你发现这是由于没有设置 FTP 站点主目录的 NTFS 权限造成的，为了让用户能够下载这些文件并最大限度地实现安全性，你应该如何设置 FTP 站点主目录的 NTFS 权限？（　　）

A．设置 Everyone 组有完全控制的权限

B．设置用户账号 IUSR_Computername 具有读取的权限

C．设置用户账号 IUSR_Computername 具有完全控制的权限

D．设置用户账号 IWAM_Computername 具有读取的权限

3．下列描述中哪个不属于 FTP 站点的安全设置？（　　）

A．读取

B．写入

C．记录访问

D．脚本访问

4．公司计划启用网站，域名为 heart.dhynet.com，服务器 IP 是 218.1.2.28，请概述完成此任务的过程。

5．公司因举行宣传活动，设计了一个新的网页，计划使用 http://heart.dhynet.com/adv 进行访问，请概述操作过程。

6．公司的宣传活动中，有一个网民参与的活动，参与者要能够以匿名登录方式把作品上传至公司的 FTP 服务器，你需要完成此任务，但还要充分考虑操作权限的安全问题。请问要如何操作？

7．为配合公司的活动要求，你搭建了 FTP 服务器，并将目录定位到了 NTFS 文件格式的磁盘下，你确认已经配置了 FTP 的写入权限，但在测试时发现匿名登录后，无法写入文件，请给出解决思路。

项目 6　证书服务的安装、配置与管理

通过 Internet 在网络上发送信息时，信息可能被别人截获、篡改和攻击，这种情况在需要安全保密的场合是不能允许的，如网上购物、电子银行转账汇款、秘密电子邮件通信等。如何保证电子邮件、电子商务等网络信息的安全呢？这就需要加密。证书里包含了用于加密的密钥。通过安装证书服务，能为企业提供证书服务，用户通过使用证书，可保证网上通信的安全。

知识点、技能点

- PKI 概述
- CA 服务的安装与证书申请
- 证书服务应用实例
- 证书的管理

6.1　引例：为什么要使用证书（WHY）

通过 Internet 在网络上发送信息时，信息可能被别人截获、篡改和攻击，这种情况在需要安全保密的场合是不能允许的，如网上购物、电子银行转账汇款、秘密电子邮件通信等。如何保证电子邮件、电子商务等网络信息的安全呢？这就需要加密。证书里包含了用于加密的密钥。

6.2　案例：构建 SSL 安全网站连接

6.2.1　工作情景描述

DHYNET 公司建立了自己的网站，希望事业合作伙伴、供货商、客户等能够安全地通过 Internet 访问这个网站，这里的安全包括：一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性，防止钓鱼网站。

6.2.2　案例分析

DHYNET 公司希望在各分公司、事业合作伙伴、供货商和客户之间，能够安全地通过 Internet 访问自己的网站，实质上就是要求对发送的信息要加密。要加密就要使用证书。有的政府机构和商业公司提供证书服务，但那是要收费的。如果想为公司节省下这笔费用，可以利用 Windows Server 2008 提供的证书服务自己搭建证书颁发机构（CA），然后为公司员工、客户供货商等颁发证书，设置他们使用的计算机信任该 CA，就能够安全地通过 Internet 发送和接受信息了。

6.2.3　相关知识

1．电子交易的网络安全问题

概括起来，进行电子交易的因特网用户所面临的安全问题有以下几点。

1）保密性

如何保证电子商务中涉及的大量保密信息在公开网络的传输过程中不被窃取，如你的电子

银行账号和密码、你的邮箱账号和密码等。

2）完整性

如何保证电子商务中所传输的交易信息不被中途篡改并通过重复发送进行虚假交易，如转账 1 000 元被别人修改成 10 000 元，或者反过来 10 000 元被改成 1 000 元。

3）身份认证与授权

在电子商务的交易过程中，如何对双方进行认证，以保证交易双方身份的正确性，如甲要转账给乙，却错误地转给了丙。

4）抗抵赖

在电子商务的交易完成后，如何保证交易的任何一方无法否认已发生的交易。

这些安全问题将在很大程度上限制电子商务的进一步发展，因此如何保证 Internet 网上信息传输的安全，已成为发展电子商务的重要环节。

上面的第一个问题是加密问题，第二、三、四个问题是签名问题，公开密钥密码体制很好地解决了这两个问题，下面介绍公开密钥密码体制、加密，以及签名的原理。

2．公开密钥密码体制

有两种密钥体制，对称密钥体制和公开密钥体制（又称非对称密钥体制），对称密钥体制的加密密钥和解密密钥是相同的，公开密钥体制的加密密钥和解密密钥是不同的。

密钥在基于公开密钥密码体制的安全系统中是成对生成的，每对密钥由一个公钥 PK 和一个私钥 SK 组成。公钥和私钥就像锁和钥匙。在实际应用中，私钥由拥有者自己保存，而公钥则需要公布于众。如果 A 向 B 发送加密文件，就使用 B 的公钥 PKB 对明文 X 进行 E 运算，得出密文 Y；B 收到密文 Y 后，使用自己对应的私钥 SKB 对密文 Y 进行 D 运算，得出明文 X。如果 A 向 B 发送签名文件，就使用 A 自己的私钥 SKA 对明文 X 进行 D 运算，得出密文 Y；B 收到密文 Y 后，使用 A 的对应的公钥 SKA 对密文 Y 进行 E 运算，得出明文 X。

3．公钥基础结构（PKI）简介

PKI（Pubic Key Infrastructure）是一种遵循标准的、利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。PKI 的核心组成部分 CA（Certification Authority），即认证中心，它是数字证书的签发机构。数字证书，有时被称为数字身份证，是一个符合一定格式的电子文件，用来识别电子证书持有者的真实身份。

前面说到，可以使用公钥和私钥进行加密和签名，并用相对应的私钥和公钥进行解密和验证签名。但是现在又产生了一个新的问题，即如何才能确定这个公钥就是某个人的。假如我们得到了一个虚假的公钥，比如说我们想传给 A 一个文件，于是开始查找 A 的公钥，但是这时 B 从中捣乱，用他自己的公钥替换了 A 的公钥，让我们错误地认为 B 的公钥就是 A 的公钥，导致我们最终使用 B 的公钥加密文件，结果 A 无法打开文件，而 B 可以打开文件，这样 B 就实现了对保密信息的窃取行为。因此就算是采用非对称密码技术，我们仍旧无法保证保密性的实现，那我们如何才能确切地得到我们想要的人的公钥呢？这时我们很自然地想到需要一个仲裁机构，或者说是一个权威的机构，它能为我们准确无误地提供我们需要的人的公钥，这个机构就是 CA。

这实际上也是应用公钥技术的关键，即如何确认某个人真正拥有公钥（及对应的私钥）。在 PKI 中，为了确保用户的身份及他所持有密钥的正确匹配，公开密钥系统需要一个值得信赖且独立的第三方机构充当认证中心（Certification Authority，CA），来确认公钥拥有人的真正身份。就像公安局发放的身份证一样，认证中心发放一个叫“数字证书”的身份证明。

这个数字证书包含了用户身份的部分信息及用户所持有的公钥。像公安局对身份证盖章一

样，认证中心利用本身的私钥为数字证书加上数字签名。任何想发放自己公钥的用户，可以去认证中心申请自己的证书。认证中心在鉴定该人的真实身份后，颁发包含用户公钥的数字证书。其他用户只要能验证证书是真实的，并且信任颁发证书的认证中心，就可以确认用户的公钥。认证中心是公钥基础设施的核心，有了大家信任的认证中心，用户才能放心方便地使用公钥技术带来的安全服务。

6.3　案例实施过程

6.3.1　任务 1：安装证书服务并架设企业根

证书颁发机构（CA）接受证书申请，根据 CA 的策略验证申请者的信息，然后使用其私钥将其数字签名应用于证书。然后 CA 将证书颁发给证书的使用者，在公钥基础结构（PKI）内用做安全凭证。此外，CA 还负责吊销证书和发布证书吊销列表（CRL）。

CA 可以是外部公司（如 VeriSign）提供的，但是要交费才能获得服务；也可以通过安装 Active Directory 证书服务（ADCS）而创建公司自己的 CA。每个 CA 都要求证书申请者有明确的身份证明，如域账户、员工的工作证、驾照、已确认的申请或物理地址。与此类似的身份检查通常要现场进行，以便公司能够验证它们自己的员工或成员。

Microsoft 企业 CA 使用个人的用户账户凭据作为身份证明。换句话说，如果您登录到一个域并申请企业 CA 的证书，则 CA 可以根据您在 Active Directory 域服务（ADDS）中的账户对您的身份进行验证。

每个 CA 还有确认自己身份的证书，该证书由另一个受信任的 CA 颁发，但如果是根 CA，则由自己颁发。重要的是，任何人都可以创建 CA。因此，用户或管理员必须决定是否信任该 CA，广义来说，该 CA 所拥有的策略和过程是否适合于确认由该 CA 颁发其证书的实体的身份。

安装根 CA 的步骤如下。

（1）打开“服务器管理器”，单击“添加角色”，单击“下一步”按钮，然后单击“Active Directory 证书服务”。如图 6-1 所示，单击两次“下一步”按钮。

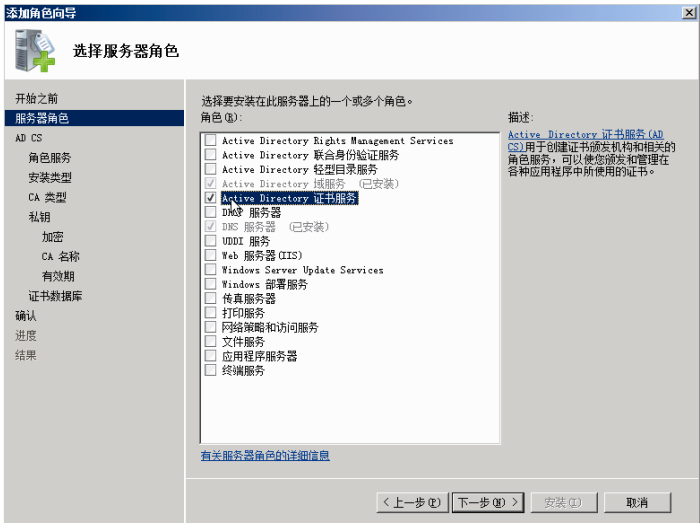

图 6-1　添加证书服务角色

（2）在“选择角色服务”页面中，确认选中“证书颁发机构”，然后选中“证书颁发机构 Web 注册”，在弹出的“添加角色向导”对话框中单击“添加必需的角色服务”按钮，然后单击“下一步”按钮，如图 6-2 所示。

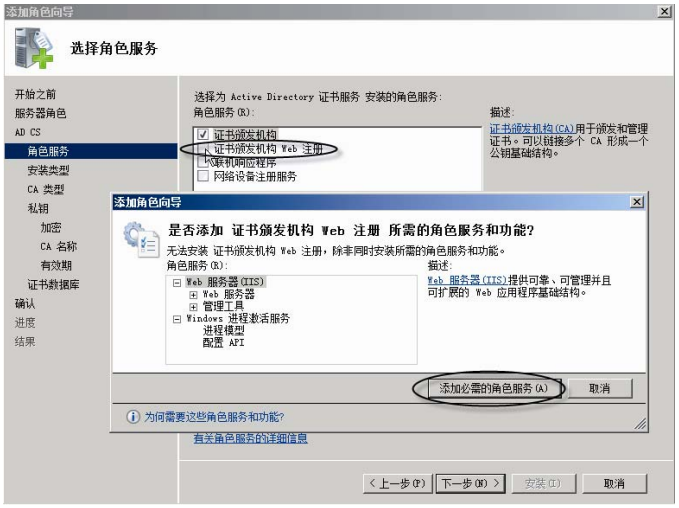

图 6-2　添加证书颁发机构注册

说明：在安装 Active Directory 证书服务时，必须安装 Web 注册支持，用户才能利用 Web 浏览器来申请证书。证书服务的 Web 注册支持可以和证书服务同时安装，也可以在证书服务安装完成后再安装。

在 Windows Server 2003 中，必须在安装证书服务之前先安装 IIS 服务，否则就无法通过 Web 注册。如果在 Windows Server 2003 中安装了证书服务后才安装 IIS 服务，则必须把证书服务卸载，然后重新安装。但在 Windows Server 2008 中已经克服了这个缺陷。

（3）在“指定安装类型”页中，单击“独立”或“企业”，这里我们选择“企业”，单击“下一步”按钮，如图 6-3 所示。

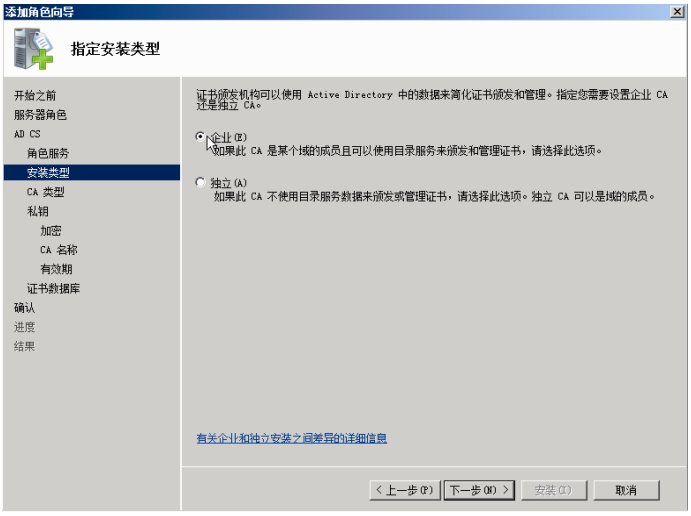

图 6-3　选择“企业”CA

注意：您的网络必须连接到域控制器，才能安装“企业”CA。

企业证书颁发机构（CA）可以通过 S/MIME（安全多用途 Internet 邮件扩展）为数字签名、为安全电子邮件颁发证书，通过安全套接字层（SSL）或传输层安全性（TLS）向安全 Web 服务器进行身份验证，通过智能卡登录到域。

企业 CA 具有以下特征。

- 需要访问 Active Directory 域服务（ADDS）。
- 使用组策略将其证书传播到域中所有用户和计算机的受信任根证书颁发机构。
- 将用户证书和证书吊销列表（CRL）发布到 ADDS。为了将证书发布到 ADDS，装有 CA 的服务器必须是 Certificate Publishers 组的成员。这对于服务器所在的域是自动进行的，但是必须为该服务器委派适当的安全权限才能向其他域发布证书。

独立 CA 具有以下特征。

- 与企业 CA 不同，独立 CA 不需要使用 Active Directory 域服务（ADDS）。即使使用 ADDS，也可以将独立 CA 用做 CA 层次结构中的脱机受信任根 CA 或通过 Extranet、Internet 向客户端颁发证书。
- 当用户向独立 CA 提交证书申请时，必须提供他们的身份信息并指定他们所需的证书类型（当向企业 CA 提交申请时，不需要执行该操作，因为企业用户的信息已经位于 ADDS 中，并且证书类型已由证书模板描述）。从本地计算机的安全账户管理器数据库中获取申请的身份验证信息。
- 默认情况下，发送到独立 CA 的所有证书申请都设置为挂起，直到独立 CA 的管理员验证了所提交的信息并批准了该申请。管理员必须执行这些任务，因为证书申请者的凭据没有经过独立 CA 的验证。
- 不使用证书模板。
- 管理员必须将独立 CA 的证书明确分发到域用户的受信任根存储，否则用户必须自己执行该任务。

安装独立 CA 与安装企业 CA 类似，本书只介绍企业 CA 的安装步骤。读者可以参考企业 CA 的安装步骤安装独立 CA。

（4）在“指定 CA 类型”页面中，单击“根 CA”，然后单击“下一步”按钮，如图 6-4 所示。

图 6-4　选择“根 CA”

根 CA 是指在组织的 PKI 中最受信任的 CA 类型。如果根 CA 被泄露或向未经授权的实体颁发了证书，则组织中任何基于证书的安全性都变得易受攻击。因此，通常根 CA 的物理安全性和证书颁发策略都比从属 CA 更严格。虽然根 CA 可以就发送安全电子邮件这样的任务向最终用户颁发证书，但是在大多数组织中，它们只用于向其他 CA（称为从属 CA）颁发证书。

从属 CA 是由组织中的另一个 CA 为其颁发的证书。通常，从属 CA 为特定用途（如安全的电子邮件、基于 Web 的身份验证或智能卡身份验证）颁发证书。从属 CA 还可以向其他更下级的从属 CA 颁发证书。根 CA、已由根验证的从属 CA，以及由其他从属 CA 验证的从属 CA 一起构成了证书层次结构。

（5）在“设置私钥”页面中，单击“新建私钥”。单击“下一步”按钮，如图 6-5 所示。

图 6-5　新建私钥

（6）在“为 CA 配置加密”页面上，选择加密服务提供程序、密钥长度和哈希算法。单击“下一步”按钮，如图 6-6 所示。

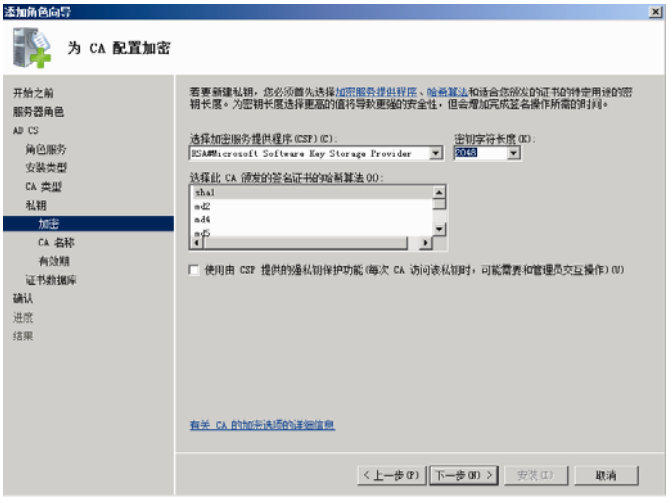

图 6-6　配置加密

选择证书颁发机构（CA）的加密选项可以显著提高 CA 的安全性、性能和兼容性。尽管默认的加密选项可能适合大多数 CA，但对于非常了解加密并且需要此灵活性的管理员和应用程序开发人员来说，执行自定义选项的能力非常有用。可以通过使用加密服务提供程序（CSP）或密钥存储提供程序执行加密选项。

CSP 是 Windows 操作系统中提供常规加密功能的硬件和软件组件。可以编写 CSP 以提供各种加密和签名算法。

在运行 Windows Vista 或 Windows Server 2008 的计算机上，密钥存储提供程序可以提供强密钥保护。

在 CA 安装过程中的“配置加密”页上，可以配置下列选项。

- “选择加密服务提供程序”。Windows Server 2008 包含很多 CSP，并且可以添加其他 CSP 或密钥存储提供程序。在 Windows Server 2008 中，提供程序列表包括算法的名称。名称中带有符号（#）的所有提供程序都是 Cryptography Next Generation（CNG）提供程序。CNG 提供程序可以支持多种非对称算法，而 CSP 只能执行一种算法。
- “密钥字符长度”。每个 CSP 都支持不同字符长度的密钥。配置较长的密钥字符长度可以增强安全性（使恶意用户更难解密密钥），但同时也会降低加密操作的性能。
- “选择用于对此 CA 颁发的证书进行签名的哈希算法”。哈希算法用于对 CA 证书和 CA 颁发的证书进行签名，以确保它们没有被篡改。每个 CSP 均可以支持不同的哈希算法。
- “使用由 CSP 提供的强私钥保护功能（可能每次 CA 访问私钥时都需要与管理员进行交互）”。要求管理员在每次加密操作之前输入密码，此选项可用于帮助阻止未经批准使用 CA 及其私钥的情况。

（7）在“配置 CA 名称”页面中，创建标识 CA 的唯一名称。单击“下一步”按钮，如图 6-7 所示。

CA 的名称长度不得超过 64 个字符，此名称将反映在 CA 颁发的每个证书中。因此，对 CA 的公用名不使用完全限定的域名非常重要。这样，获取证书副本的恶意用户将无法识别和使用 CA 的完全限定域名来制造潜在的安全漏洞。

CA 名称不必与计算机名称相同。但是，在安装 CA 之后，将无法更改服务器的名称。

若要在安装 ADCS 之后更改服务器名称，则必须卸载 CA，更改服务器的名称，重新安装 CA，然后重新颁发由 CA 颁发的所有证书。

图 6-7　配置 CA 名称

（8）在“设置有效期”页面中，指定根 CA 证书有效的年数或月数。单击“下一步”按钮，如图 6-8 所示。

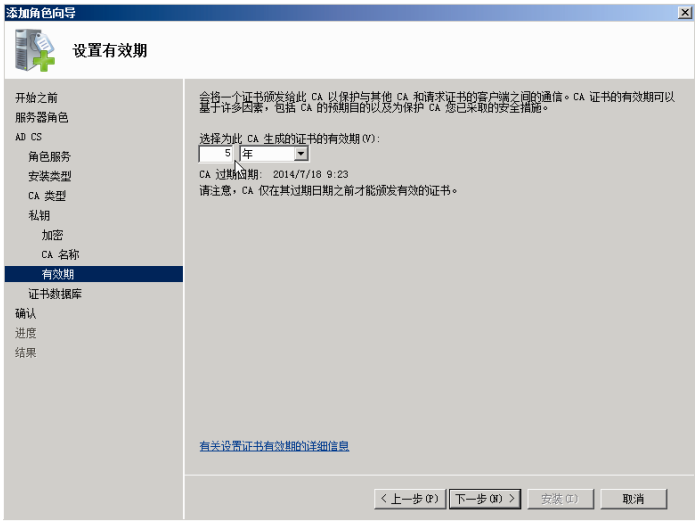

图 6-8　设置 CA 有效期

每个证书都有一个有效期。有效期过后，证书就不再被当做可接受的或可用的凭据了。

（9）在“配置证书数据库”页面上，选择保存证书数据库和证书数据库日志的适当位置。单击“下一步”按钮，如图 6-9 所示。

图 6-9　配置证书数据库

（10）在“Web 服务器（IIS）”对话框中按照默认选择，单击两次“下一步”按钮。

（11）在“确认安装选项”页面上，查看您选择的所有设置。如果要接受所有这些选项，请单击“安装”按钮，然后等待安装过程完成。

6.3.2　任务 2：为 Web 服务器创建证书申请文件

下面的步骤需要在安装 Web 服务器的计算机上进行。

（1）单击“开始”→“管理工具”→“Internet 信息服务（IIS）管理器”，在弹出的“Internet 信息服务（IIS）管理器”窗口中单击左侧窗格中的本地计算机名，双击中间窗格中的“服务器证书”，如图 6-10 所示。

图 6-10　配置服务器证书

（2）在图 6-11 中单击右侧窗格中的“创建证书申请”。

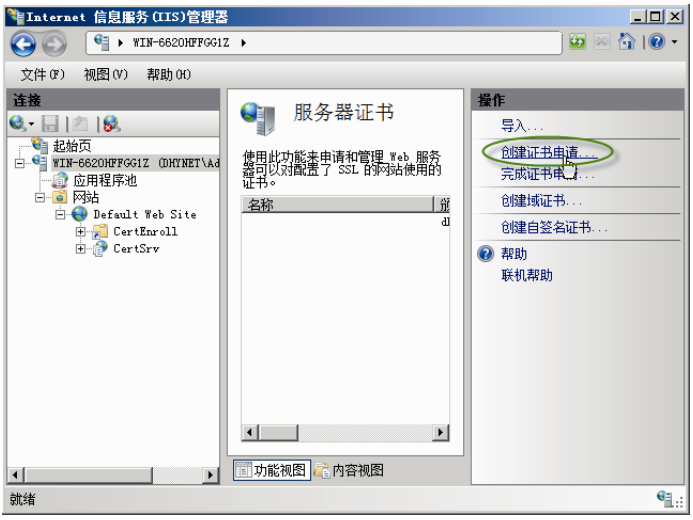

图 6-11　创建证书申请

（3）在图 6-12 中输入“通用名称”等信息。保持默认设置单击两次“下一步”按钮。

注意：“通用名称”必须与要进行加密通信的网站的名称一致。这里填写的是 DHYNET 公司的网站 www.dhynet.com，否则用户在访问网站时会看到网站的证书有问题等提示。

（4）在图 6-13 中输入证书申请文件的保存路径和文件名。单击“完成”按钮完成证书申请文件的创建。请记住你所保存的证书申请文件的路径和文件名，在下面的任务 3 中要使用。

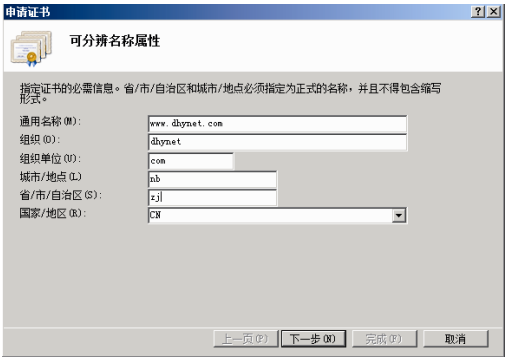

图 6-12　输入服务器信息

图 6-13　保存和命名服务器证书申请文件

6.3.3　任务 3：为 Web 服务器申请证书

下面的步骤需要在安装 Web 服务器的计算机上进行。

（1）在 Internet Explorer 中，连接到 http://servername/certsrv，其中 servername 是安装 CA 的服务器的名称或者 IP 地址。本例中输入的是 http://10.1.1.100。在弹出的对话框中输入管理员用户名和密码，单击“确定”按钮，如图 6-14 所示。

（2）如果弹出如图 6-15 所示的提示对话框，则单击“添加”按钮，把 http://10.1.1.100 添加到可信任站点中。

图 6-14　连接 CA 服务器

图 6-15　添加 CA 服务器为可信任站点

（3）在图 6-16 中单击“申请证书”。

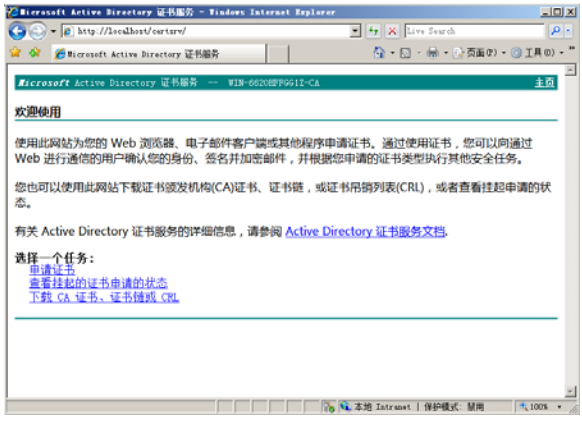

图 6-16　申请证书

（4）在图 6-17 中。单击“高级证书申请”。

图 6-17　高级证书申请

（5）系统弹出如图 6-18 所示的窗口。单击“使用 base64 编码的 CMC 或 PKCS#10 文件提交一个证书申请，或使用 base64 编码的 PKCS#7 文件续订证书申请”。

图 6-18　选择高级证书申请的类别

（6）打开在任务 2 中保存的证书申请文件，把文件内容全部复制到“保存的申请”文本框中；在“证书模板”下拉列表中选择“Web 服务器”，单击“提交”按钮，如图 6-19 所示。

（7）在图 6-20 中单击“下载证书”。把证书保存在安全适当的地方。关闭 IE 浏览器。

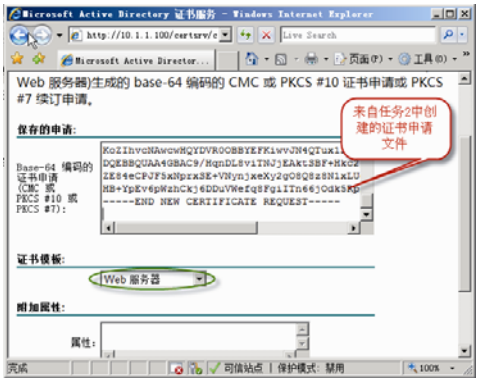

图 6-19　输入证书相关信息

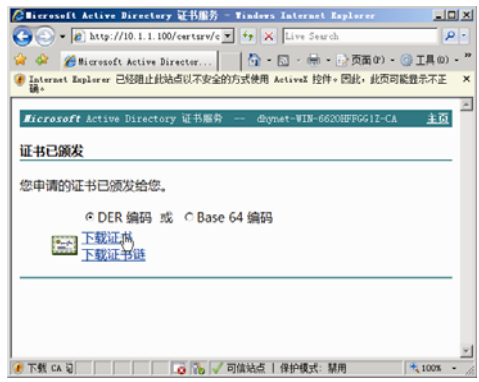

图 6-20　下载证书

6.3.4　任务 4：为 Web 服务器完成证书申请

下面的步骤需要在安装 Web 服务器的计算机上进行。

（1）单击“开始”→“管理工具”→“Internet 信息服务（IIS）管理器”，在弹出的“Internet 信息服务（IIS）管理器”窗口中单击左侧窗格中的本地计算机名，双击中间窗格中的“服务器证书”，如图 6-21 所示。

图 6-21　IIS 管理器

（2）单击右侧窗格中的“完成证书申请”，如图 6-22 所示。

（3）在图 6-23 中输入任务 3 中为 Web 服务器申请的证书的保存路径和文件名，并输入一个好记的名称，单击“确定”按钮。

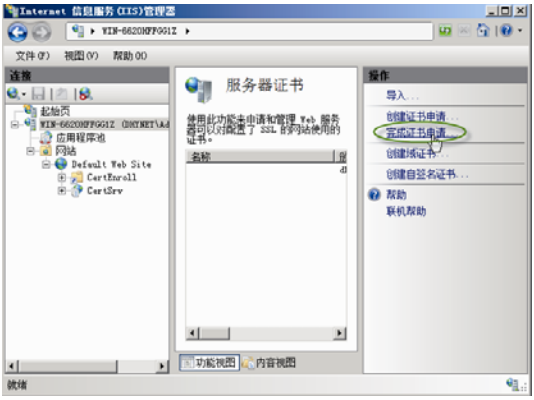

图 6-22　选择完成证书申请

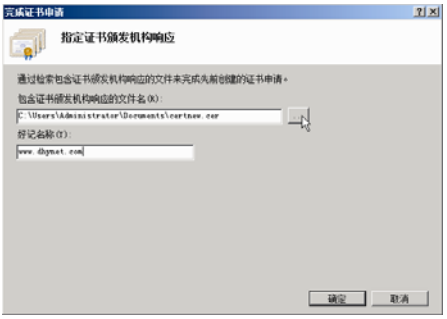

图 6-23　选择申请到的证书

6.3.5　任务 5：为 Web 服务器绑定证书并启用 SSL

下面的步骤需要在安装 Web 服务器的计算机上进行。

（1）单击“开始”→“管理工具”→“Internet 信息服务（IIS）管理器”，在弹出的“Internet 信息服务（IIS）管理器”窗口中找到要加密浏览的网站，如本例中的“www.dhynet.com”，单击网站，单击右侧窗格中的“绑定”，如图 6-24 所示。

（2）在图 6-25 中单击“添加”按钮。在打开的“添加网站绑定”对话框中进行设置，“类型”选择“https”，“SSL 证书”选择“www.dhynet.com”，证书“www.dhynet.com”是在任务 4 中输入的那个证书的好记的名称。单击“确定”和“关闭”按钮。

图 6-24　绑定证书

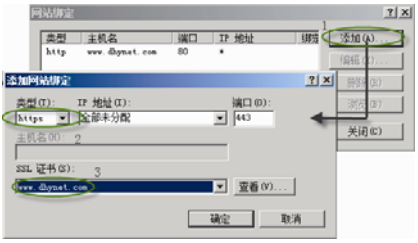

图 6-25　选择证书

（3）在“Internet 信息服务（IIS）管理器”窗口中，确认选中了“www.dhynet.com”，然后双击中间窗格中的“SSL 设置”，如图 6-26 所示。

（4）在图 6-27 中勾选中间窗格中的“要求 SSL”，并单击右侧窗格中的“应用”。

图 6-26　启用 SSL 设置

图 6-27　应用 SSL 设置

6.3.6　任务 6：验证加密访问

首先，设置计算机信任 CA。如果计算机尚未信任一个 CA，那么就会显示如图 6-28 所示的“此网站的安全证书有问题”的提示。

下面在一台 Windows 7 计算机中验证是否能够进行加密访问。

（1）通过浏览器连接到 CA，选择“下载 CA 证书，证书链或 CRL”，如图 6-29 所示。

（2）选择“下载 CA 证书链”，如图 6-30 所示。把下载的 CA 证书链保存在安全的地方。

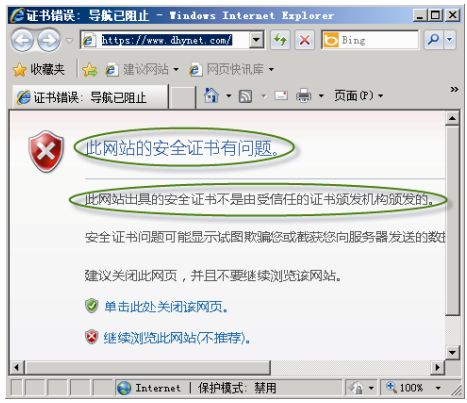

图 6-28　计算机不信任 CA 时的提示

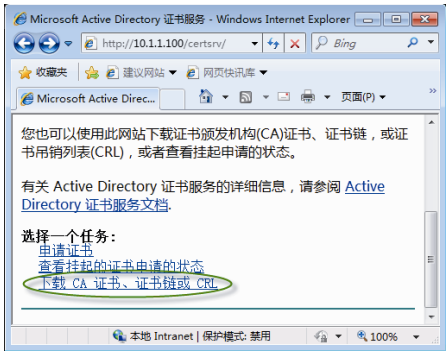

图 6-29　连接到 CA

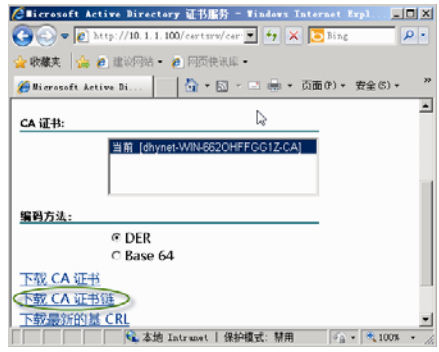

图 6-30　下载 CA 证书链

（3）把下载的 CA 证书链导入到受信任的根证书颁发机构。在 IE 浏览器中单击“工具”→“Internet 选项”→“内容”→“证书”→“受信任的根证书颁发机构”，系统弹出如图 6-31 所示的“证书”对话框，单击“导入”按钮。

（4）根据提示把步骤（2）中下载的证书链导入。

（5）在 IE 的地址栏中输入 https://www.dhynet.com，应该能够正确访问，如图 6-32 所示。

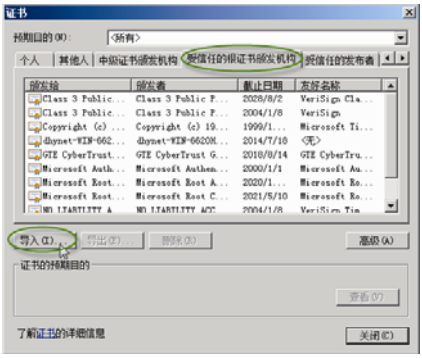

图 6-31　导入到受信任的根证书颁发机构

图 6-32　正确访问

（6）在 IE 的地址栏中输入“https://10.1.1.100”，10.1.1.100 是 www.dhynet.com 站点的 IP 地址。系统会显示“此网站的安全证书有问题”，如图 6-33 所示。造成这种情况的原因是，在提供的证书申请信息中，通用名称是 www.dhynet.com，用户必须输入“https://www.dhynet.com”才能正确显示。

（7）下面进一步设置网站的 SSL 属性。单击“开始”→“管理工具”→“Internet 信息服务（IIS）管理器”。在图 6-34 中选中要设置的网站，如本例中的“www.dhynet.com”，然后在中间窗格中双击“SSL 设置”。

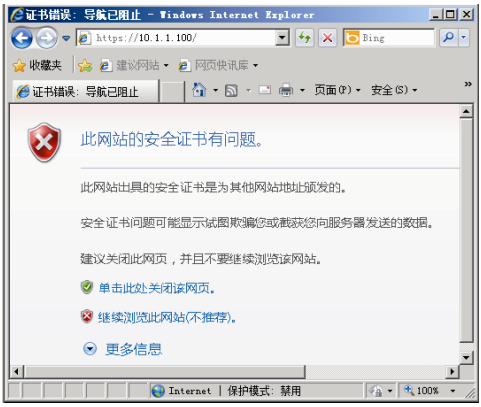

图 6-33　网站的安全证书有问题的提示

图 6-34　进一步设置 SSL 属性

（8）在图 6-35 中选中“要求 SSL”和“客户证书”选项中的“必需”。

（9）再一次在 Windows 7 计算机中访问“https://www.dhynet.com”，可以看到出现如图 6-36 所示的情况，即拒绝访问。这是因为在 Windows 7 中的用户还没有申请数字证书。注意，此步骤可能需要重启 IE。

图 6-35　设置客户证书“必需”

图 6-36　客户没有证书时的提示信息

（10）在 Windows 7 中申请客户端证书。具体申请的方法见 6.3.7 小节的相关内容。申请并安装证书后，再次访问 https://www.dhynet.com，如图 6-37 所示，需要确认证书，单击“确定”按钮，就可以正常访问了。注意，此步骤可能需要重启 IE。

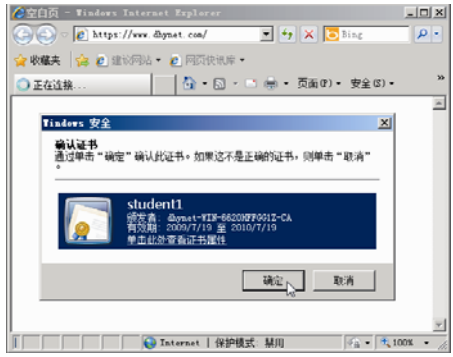

图 6-37　客户申请证书后的访问情况

通过本任务可以看出，通过使用证书，既能对访问网站时传输的数据进行加密，还能限制用户的访问，只有获取证书的用户才能访问网站的资源。这样就在一定程度上保证了公司数据的安全。

6.3.7　任务 7：域用户如何向企业 CA 申请证书

用户可以通过以下方式获取证书。

1．使用证书申请向导申请证书

下面以加入域的 Windows 7 操作系统为例进行讲述。

（1）域用户 student-1 从安装有 Windows 7 操作系统的计算机登录后，单击“开始”→“所有程序”→“附件”→“运行”，在“运行”对话框中输入“mmc”，单击“确定”按钮。在弹出的控制台中单击菜单“文件”→“添加/删除管理单元”，在“添加或删除管理单元”对话框中选中“证书”，单击“添加”按钮。单击“确定”按钮，打开用户或计算机的“证书”管理单元，如图 6-38 所示。

（2）在控制台树中，单击“证书-当前用户”或“证书（本地计算机）”，选择“个人”，如图 6-39 所示。

图 6-38　添加证书管理单元

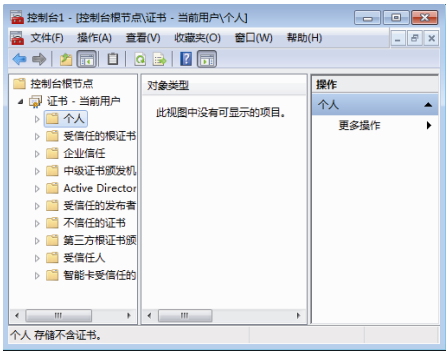

图 6-39　选择证书保存的位置

（3）在“操作”菜单上，指向“所有任务”，然后单击“申请新证书”，如图 6-40 所示，从而启动证书注册向导，单击“下一步”按钮。

（4）选择证书注册策略，本例选中默认的“由管理员配置”下的“Active Directory 注册策略”，如图 6-41 所示。单击“下一步”按钮。

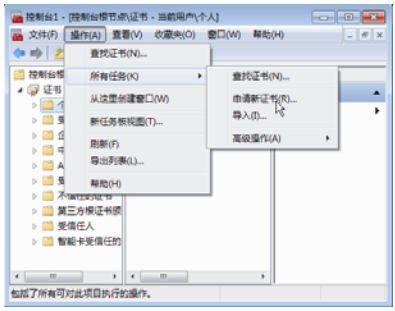

图 6-40　申请新证书

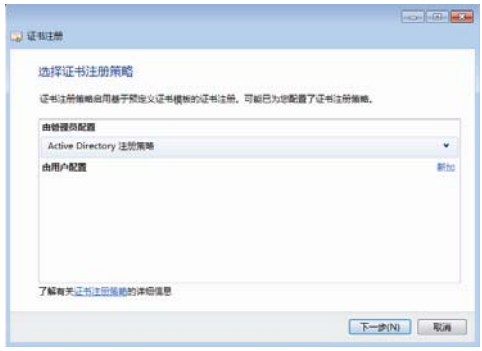

图 6-41　选择证书注册策略

（5）选择证书的类型。证书的类型不同，用途也不同。单击“详细信息”可以查看每个证书的详细信息，如图 6-42 所示。

如果证书下方出现警告符号，则可能需要在申请该类型证书之前提供其他信息。

图 6-42　选择证书的类型

（6）设置完成，请单击“注册”按钮，然后在图 6-43 中单击“完成”按钮。

（7）在证书管理单元中，展开“个人”→“证书”，可以看到刚才申请的两个证书，如图 6-44 所示。

图 6-43　注册完成

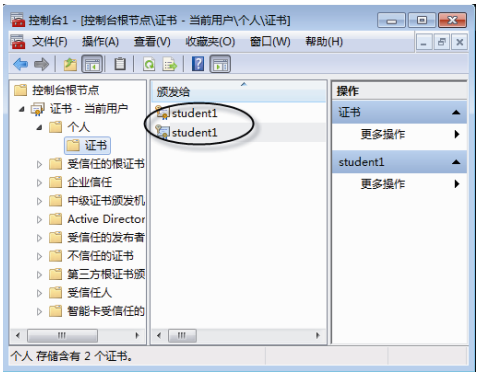

图 6-44　申请到的证书

2．自动注册证书

证书最常见的用途就是允许使用者使用自动注册功能进行注册。在这种情况下，使用者必

须被授予“读取”、“注册”和“自动注册”权限。

设置自动证书注册的主要步骤如下。

- 在证书服务器上复制并添加允许自动注册的证书模板。
- 在证书服务器上设置证书自动模板允许用户自动注册。
- 在域控制器上为域配置自动注册组策略。
- 在客户机上用户通过证书管理单元自动注册证书。

下面逐项说明其实施的步骤。

下面的步骤说明如何在证书服务器上复制并添加允许自动注册的证书模板。这些步骤要在证书服务器上完成。

（1）打开“服务器管理器”，如图 6-45 所示展开到“证书模板”，在中间窗格中右击要允许为自动注册的模板，如“用户”模板，选择“复制模板”。

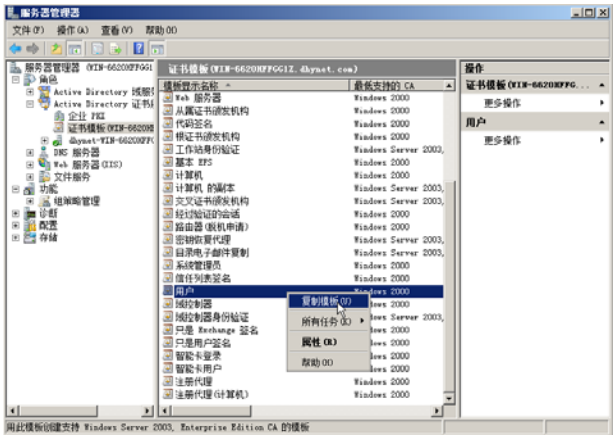

图 6-45　复制证书模板

（2）在“复制模板”对话框中选择默认的支持证书模板的 Windows Server 版本，单击“确定”按钮，如图 6-46 所示。

（3）在“新模板的属性”的“常规”选项卡中修改“模板显示名称”为合适的名称，如“公司用户”，如图 6-47 所示。

图 6-46　选择默认的支持证书模板的 Windows Server 版本

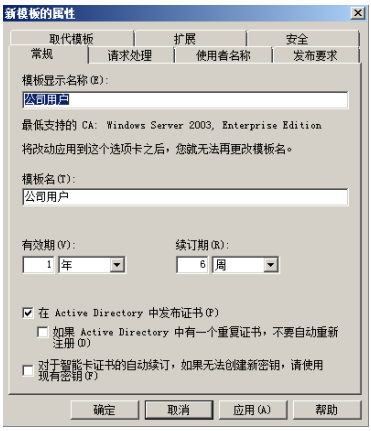

图 6-47　修改“模板显示名称”

（4）在“新模板的属性”的“安全”选项卡中，选中“组或用户名”中的“Domain Users”，在“Domain Users 的权限”中设置允许“读取”、“注册”和“自动注册”。用户必须要有自动注册的权限才能自动注册证书。单击“确定”按钮，如图 6-48 所示。

（5）在图 6-49 中展开到“证书模板”（注意图中有两个证书模板），右击“证书模板”，选择“新建”→“要颁发的证书模板”。

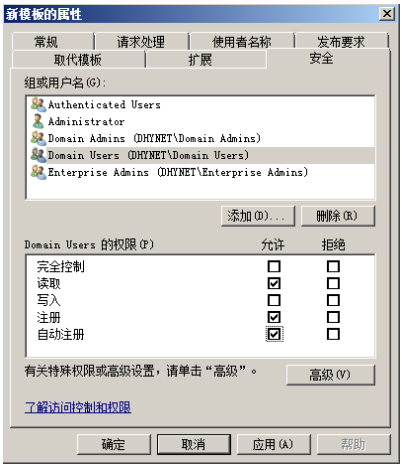

图 6-48　设置允许“自动注册”

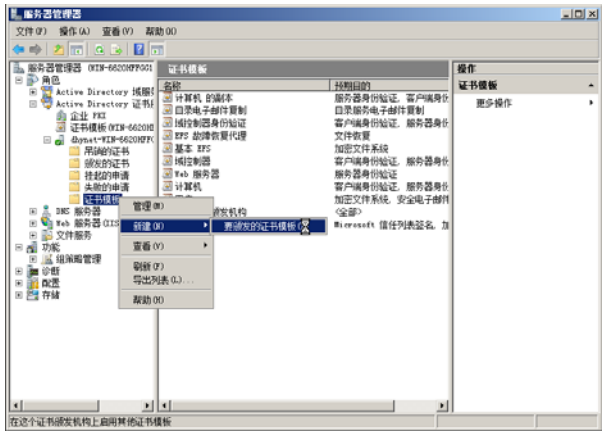

图 6-49　新建要颁发的证书模板

（6）在图 6-50 中选中要启用的证书模板“公司用户”，单击“确定”按钮。这时在证书模板中就新添加了“公司用户”模板。

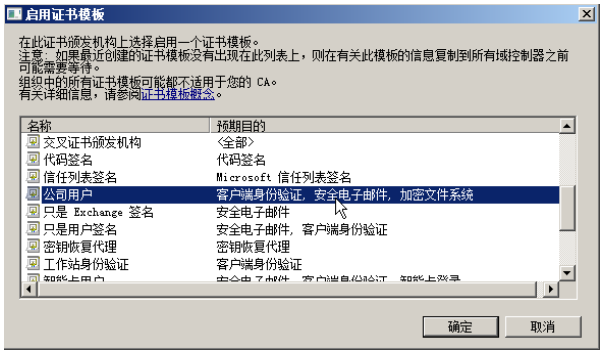

图 6-50　选中要启用的证书模板

下面的步骤说明如何为域配置组策略，以允许用户自动注册证书。这些步骤要在域控制器上完成。

Domain Admins 或 Enterprise Admins 中的成员身份或等效身份是完成此过程所需的最低要求。

（7）在运行 Windows Server 2008 的域控制器上，单击“开始”，指向“管理工具”，然后单击“组策略管理”。

在控制台树中，右击“Default Domain Policy”，然后单击“编辑”，如图 6-51 所示。

（1）在组策略管理编辑器控制台（GPMC）中，依次展开“用户配置”→“策略”→“Windows 设置”→“安全设置”→“公钥策略”，如图 6-52 所示。

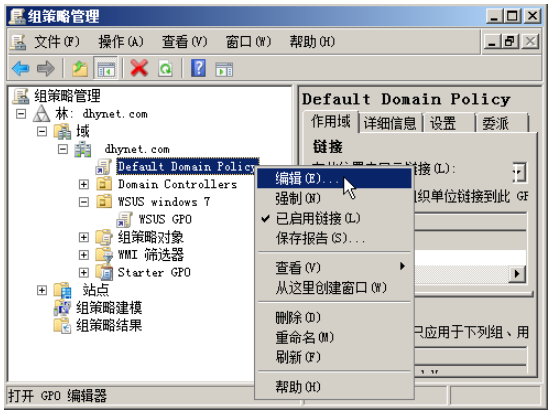

图 6-51　打开组策略

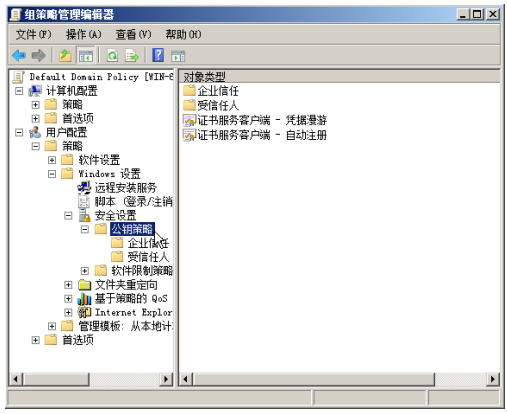

图 6-52　找到并展开“公钥策略”

（2）在图 6-52 中双击“证书服务客户端 - 自动注册”，弹出如图 6-53 所示的对话框，在“配置型号”中选择“已启用”。单击“确定”按钮接受更改。

下面的步骤说明如何使用“证书”管理单元自动注册证书。这些步骤要在客户机上完成。用户或本地管理员是完成此过程所需的最低组成员身份。

（1）打开用户或计算机的“证书”管理单元。

在控制台树中，单击“证书-当前用户”或“证书（本地计算机）”。

在“操作”菜单上，指向“所有任务”，然后单击“自动注册并检索证书”，如图 6-54 所示。

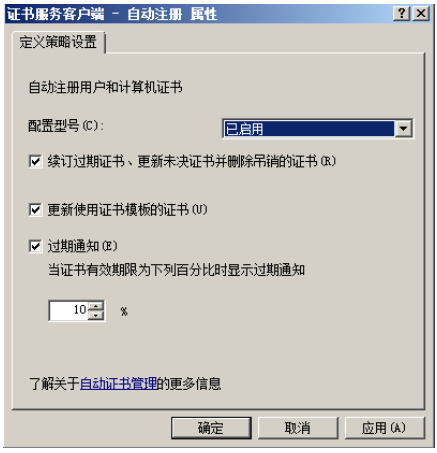

图 6-53　启用证书服务客户端自动注册

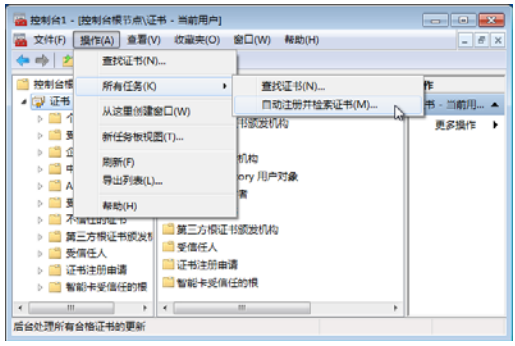

图 6-54　客户端自动注册证书

（2）单击“下一步”按钮。选择要获取的证书“公司用户”，然后单击“注册”按钮，如图 6-55 所示。完成注册处理时，单击“完成”按钮。

注意：因为用户证书的功能之一是为用户的电子邮件加密，所以在这个步骤之前，应确保已为该域用户设置了电子邮箱，否则无法申请成功。

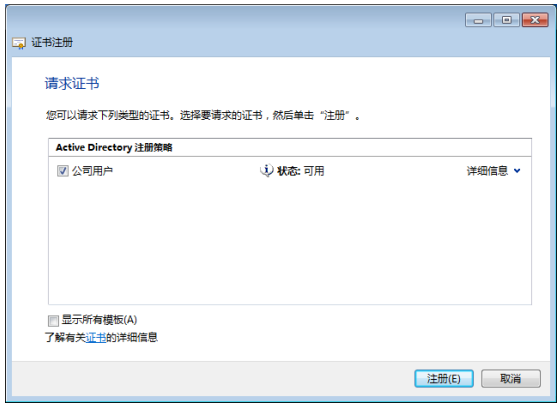

图 6-55　自动注册完成

3．利用 Web 浏览器来申请证书

在前面已经讲过如何利用 Web 浏览器为 Web 服务器来申请证书，用户利用 Web 浏览器来申请证书与为 Web 服务器申请证书基本一致，不同的是申请的证书类型不同，用户申请的是用户证书。

下面的步骤在 Windows 7 操作系统中完成，以用户 student1 的身份登录。

（1）打开 Internet Explorer。

（2）在 Internet Explorer 中，连接到 https://servername/certsrv，其中 servername 是安装 CA 的服务器的名称。本例中输入的 https:// win-662ohffgg1z /certsrv 中 win-662ohffgg1z 即是 CA 服务器的计算机名。

单击“申请证书”，如图 6-56 所示。

图 6-56　单击“申请证书”

注意：

- 这里并没有要求用户输入用户验证信息，因为用户是以域用户 student1 的身份登录的。如果不是以域用户的身份登录，系统会弹出对话框要求用户输入要申请证书的用户名和密码。

- 证书申请要求使用安全的 https 连接，此时 Active Directory 证书服务器必须进行了 SSL 设置。如果 Active Directory 证书服务器没有进行 SSL 设置，则必须设置 IE 浏览器中的 Internet 选项的安全设置。具体操作步骤是，打开 IE 浏览器，单击菜单“工具”→“Internet 选项”→“安全”→“本地 Intranet”，设置该区域的安全级别为“低”。如图 6-57 中的 1、2 所示。单击“站点”，弹出“本地 Intranet”对话框，输入 http://CA 的 IP 地址或域名，如 http://10.1.1.100，然后单击“添加”按钮，确认没有勾选“对该区域中的所有站点要求服务器验证（https）”，然后单击“关闭”、“确定”按钮，如图 6-57 中的 3、4、5、6、7 所示。这样做也可以申请证书，但增加了申请证书过程中的安全风险。

图 6-57　降低浏览器安全级别

（3）在“申请证书”中，选择所需证书的类型。

- 如果 CA 是企业 CA，请单击“用户证书”。
- 如果 CA 是独立 CA，请选择“Web 浏览器证书”或“电子邮件保护证书”。

如果需要，可在“识别信息”页面上，输入用于证书申请的识别信息。

这里单击“用户证书”，如图 6-58 所示。

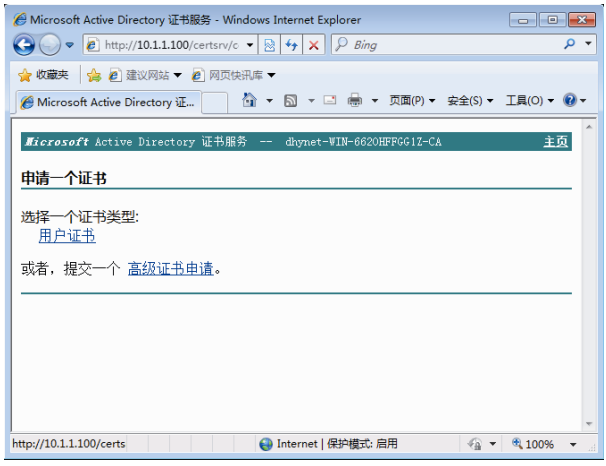

图 6-58　申请用户证书

（可选）单击“更多选项”以指定加密服务提供程序（CSP），以及是否要启用强私钥保护（这意味着每次使用与证书相关的私钥时，您都将收到提示消息）。

（4）在图 6-59 中的“Web 访问确认”对话框中单击“是”按钮，然后单击“提交”按钮。

（5）在图 6-60 中的“Web 访问确认”对话框中单击“是”按钮，然后单击“安装此证书”。

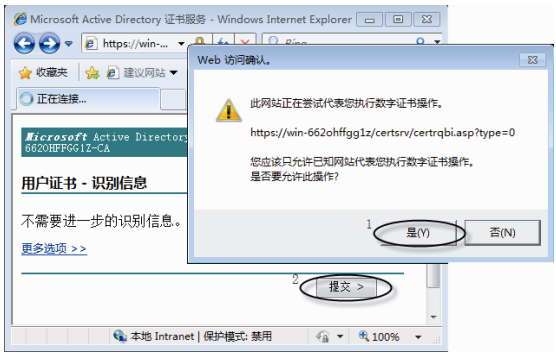

图 6-59　提交申请

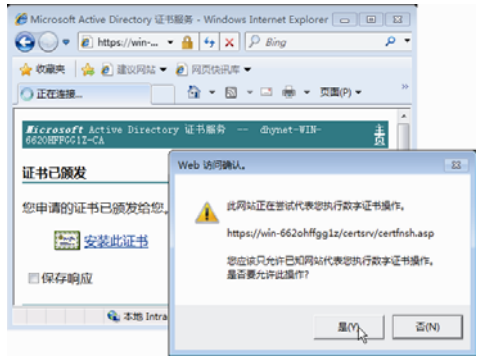

图 6-60　安装证书

注意：这个例子是向企业根申请证书，如果是向独立根申请证书，证书不会自动颁发，需要等待独立证书服务器颁发后才能查看和安装。

（6）安装完成后，可以查看所安装的证书。在 IE 中单击“工具”→“Internet 选项”，在弹出的对话框的“内容”选项卡中单击“证书”按钮，可以看到所申请的证书，如图 6-61 所示。在这个页面中也可以导入导出证书。读者可以自己摸索一下。如果使用网页完毕，请关闭 Internet Explorer。

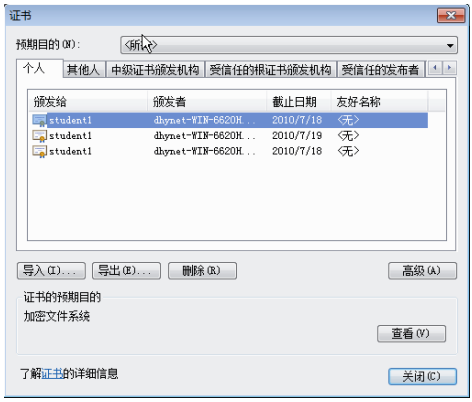

图 6-61　查看证书

6.4　知识能力拓展

6.4.1　证书管理：导出与导入

出于保存证书的需要，可以导出证书保存在一个安全的地方；反之，如果需要，可以从保存的地方把证书导入到需要的地方。

在 Windows Server 2008 中，不能直接申请计算机证书，需要把申请到的用户证书导出，然后再导入到计算机账户。

（1）添加管理单元。单击“开始”→“运行”，输入 mmc 并回车，在弹出的控制台中单击“文件”菜单，选中“添加/删除管理单元”，如图 6-62 所示。

（2）添加用户账户证书管理单元。在图 6-63 中依次单击标注 1、2、3 所指的“证书”、“添加”、“我的用户帐（账）户”，然后单击“完成”按钮。

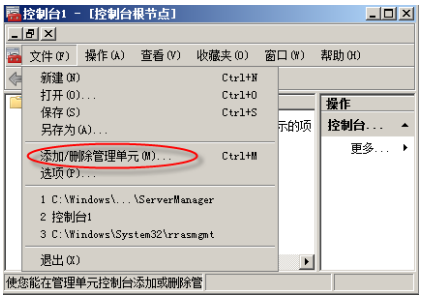

图 6-62　打开 mmc

图 6-63　添加用户账户证书管理单元

（3）添加计算机账户证书管理单元。在图 6-64 中依次单击标注 1、2、3 所指的“证书”、“添加”、“计算机账户”，然后单击“下一步”按钮。

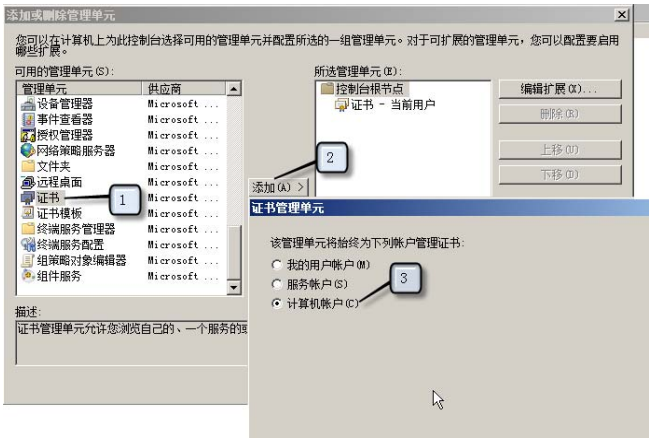

图 6-64　添加计算机账户证书管理单元

（4）在图 6-65 中确认选中了“本地计算机”，然后单击“完成”按钮，再单击“确定”按钮。

（5）在控制台中依次展开“证书-当前用户”→“个人”→“证书”，在中间窗格中右击证书，选中“所有任务”→“导出”，如图 6-66 所示。单击“下一步”按钮。

（6）在图 6-67 中选中“是，导出私钥”，单击两次“下一步”按钮。

（7）在图 6-68 中输入保护私钥的密码，单击“下一步”按钮。

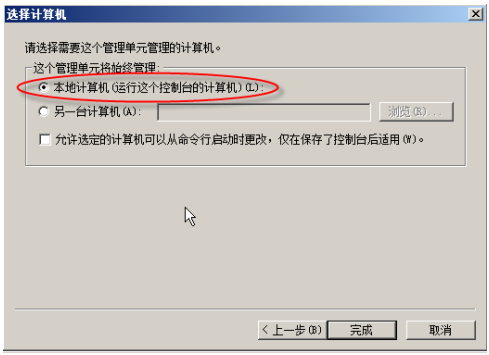

图 6-65　确认选中了“本地计算机”

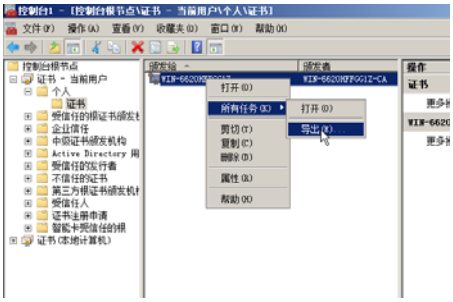

图 6-66　导出证书

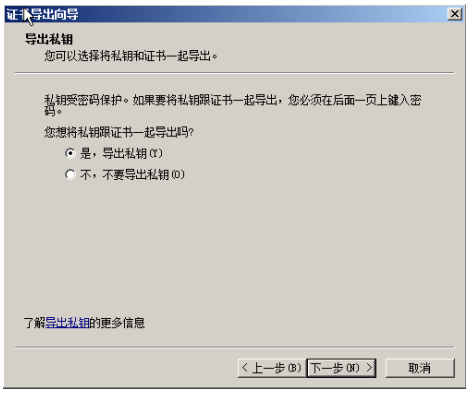

图 6-67　导出私钥

图 6-68　输入保护私钥的密码

（8）在图 6-69 中输入保存证书的路径和文件名，或者单击浏览找到合适的路径并输入保存证书的文件名。单击“下一步”按钮，再单击“完成”和“确定”按钮。

（9）把从用户账户中导出的证书导入到计算机账户中。在控制台中依次展开“证书（本地计算机）”→“个人”→“证书”，右击“证书”，选中“所有任务”→“导入”，如图 6-70 所示。单击“下一步”按钮。

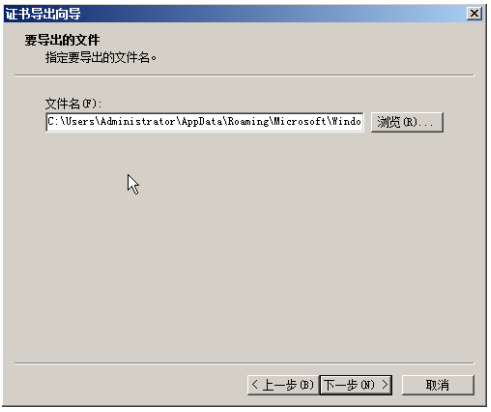

图 6-69　输入保存证书的路径和文件名

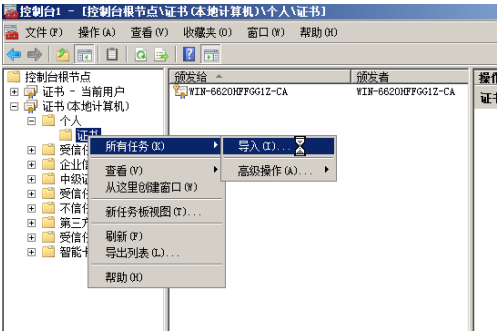

图 6-70　导入证书

（10）在图 6-71 中输入要导入的证书的路径和文件名，单击“下一步”按钮。

（11）在图 6-72 中输入保存证书时输入的保护私钥的密码，单击两次“下一步”按钮，再单击“完成”和“确定”按钮。

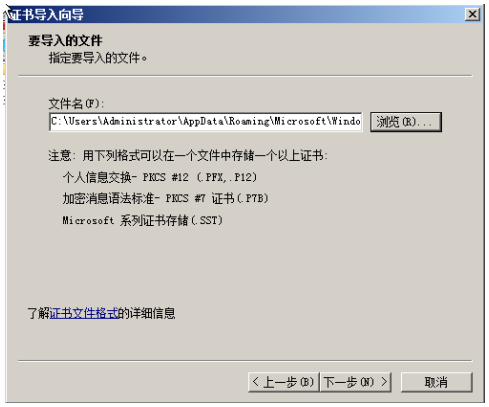

图 6-71　输入要导入的证书的路径和文件名

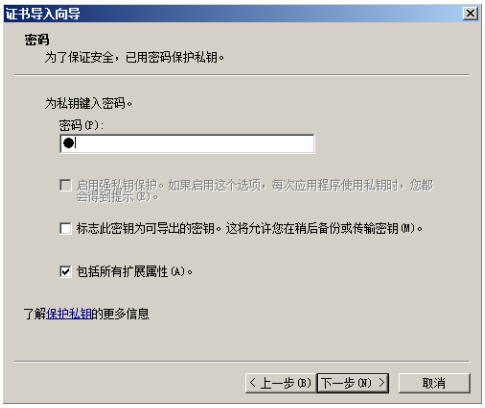

图 6-72　输入密码

6.4.2　企业从属 CA 的安装

（1）打开“服务器管理器”，单击“添加角色”，单击“下一步”按钮，然后单击“Active Directory 证书服务”。单击两次“下一步”按钮。

（2）在“选择角色服务”页上，单击“证书颁发机构”，然后单击“下一步”按钮。

（3）在“指定安装类型”页面上，单击“独立”，然后单击“下一步”按钮。

您的网络必须连接到域控制器，才能安装企业 CA。

（4）在“指定 CA 类型”页上，单击“从属 CA”，然后单击“下一步”按钮。

（5）在“设置私钥”页上，单击“新建私钥”，然后单击“下一步”按钮。

（6）在“配置加密”页面上，选择加密服务提供程序、密钥长度和哈希算法，然后单击“下一步”按钮。

（7）在“申请证书”页上，浏览到根 CA，如果根 CA 没有连接到网络，则将证书申请保存到文件中，以便以后进行处理。单击“下一步”按钮。

注意：

发布了根 CA 证书并且使用该证书完成从属 CA 的安装之后，才能使用从属 CA。

（8）在“配置 CA 名称”页面中，创建标识 CA 的唯一名称。单击“下一步”按钮。

（9）在“设置有效期”页面中，指定 CA 证书有效的年数或月数。单击“下一步”按钮。

（10）在“配置证书数据库”页面上，选择要保存的位置。单击“下一步”按钮。

（11）在“确认安装选项”页面上，查看您选择的所有配置。如果接受所有这些选项，请单击“安装”按钮，然后等待安装过程完成。

6.4.3　证书颁发机构的备份与还原

证书颁发机构（CA）是任何组织的重要资源。因此，定期备份和还原非常重要。

可以备份证书颁发机构（CA）而不必备份在其上安装 CA 的整个服务器。但是，多数情况下应使用备份管理单元同时备份和还原 CA 和服务器。

您必须是 CA 管理员或 Backup Operators 组的成员或具有同等身份，才能完成此过程。

1．使用证书颁发机构管理单元备份 CA 的步骤

（1）打开“证书颁发机构”管理单元。

（2）在控制台树中，单击 CA 的名称。

（3）在“操作”菜单上，指向“所有任务”，单击“备份 CA”。

（4）按照 CA 备份向导中的指示操作。

2．使用证书颁发机构管理单元从备份副本还原 CA 的步骤

（1）打开“证书颁发机构”管理单元。

（2）在控制台树中，单击 CA 的名称。

（3）在“操作”菜单上，指向“所有任务”，单击“还原 CA”。

（4）按照证书颁发机构还原向导中的指示操作。

6.4.4　证书的发放、吊销与更新

1．查看和发放挂起证书申请的步骤

（1）打开“证书颁发机构”管理单元。

（2）在控制台树中，单击“挂起的申请”。

（3）在详细信息窗格中，通过注释申请者姓名、申请者电子邮件地址，以及您认为能够为颁发证书提供关键信息的其他任何字段的值来检查每个证书申请。

（4）右击检查合格的证书申请，选择“发放”。

2．吊销证书的步骤

（1）打开“证书颁发机构”管理单元。

（2）在控制台树中，单击“颁发的证书”。

（3）在详细信息窗格中，单击要吊销的证书。

（4）在“操作”菜单上，指向“所有任务”，然后单击“吊销证书”。

（5）选择吊销证书的原因，调整吊销时间（如果需要），然后单击“是”。

6.5　项目完成结论

通过完成本项目，学习了如何安装证书服务、如何管理证书服务器、如何申请证书、如何管理证书，并举了一个证书的应用实例，即通过利用证书实现 Web 加密安全访问。当然证书的种类非常多，使用范围也非常广泛，限于篇幅，本章不再列举其他的应用。

6.6　练习案例

某公司搭建了 Web 服务，网站中有公司的机密内容，只希望公司内部员工访问。因此公司搭建了两个 Web 站点，一个不含机密内容，供普通用户使用，一个含有机密内容，只能内部员工访问，使用 SSL 加密，而且访问的员工必须有证书。公司自己搭建了证书服务器，为 Web 服务器颁发了证书，每个公司员工可以自动注册数字证书。根据所学的知识，实现公司的要求。

6.7　课后习题

1．公司为什么要使用证书服务？
2．证书服务有哪些类型？各有什么特点？
3．用户申请证书的方式有哪些？分别用于什么情况？
4．简述各种证书申请方式的过程。
5．在完成本章的各个案例的练习中，你遇到了哪些问题？是怎么解决的？
6．在网上查找资料，了解证书都在哪些方面使用。

项目 7　VPN 服务的安装、配置与管理

VPN 的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网络可以把它理解成是虚拟出来的企业内部专线。VPN 的核心就是利用公共网络建立虚拟私有网。虚拟专用网（VPN）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路；可用于经济有效地连接到商业伙伴。

知识点、技能点

- VPN 的基本概念
- 搭建 VPN 服务器
- 建立 VPN 客户端
- VPN 的高级设置

7.1　引例：为什么要使用远程访问服务（WHY）

公司的专用网在默认情况下是不对外开放的，也就是说，在 Internet 上是无法直接访问公司的专用网（通常就叫内网）的，这是信息安全的需要。但是，当公司员工经常出差，在出差期间需要访问公司专用网中的资源时，就希望能通过 Internet 来访问公司的专用网，这是业务的需要；再比如，公司员工在家中加班，需要访问公司专用网中的资源时，也希望能通过 Internet 来访问公司专用网。

怎么来解决上面说的信息安全和业务需要的矛盾呢？VPN 就是解决这个问题的主要方案之一。VPN 的核心就是在利用公共网络建立虚拟专用网。虚拟专用网（VPN）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

7.2　案例：建立 VPN 服务

7.2.1　工作情景描述

DHYNET 公司有员工经常出差，在出差期间需要访问公司专用网中的资源；也有公司员工在家中加班，需要访问公司专用网中的资源。但是，公司专用网的资源又不能对 Internet 开放，因为如果开放了，公司的信息安全就无从谈起了。如何既能保证公司的信息安全，又能满足员工通过 Internet 访问公司专用网中的资源的要求呢？

7.2.2　案例分析

案例中的问题是远程访问的问题，通过将“路由和远程访问”配置为充当远程访问服务器，可以将远程工作人员或流动工作人员连接到组织网络上。远程用户可以像其计算机物理连接到网络上一样进行工作。

利用远程访问连接可以使用通过 LAN 连接的用户通常可用的所有服务，包括文件共享和打印共享、Web 服务器访问和消息传递。例如，在运行“路由和远程访问”的服务器上，客户端可以使用 Windows 资源管理器来建立驱动器连接和连接到打印机。由于远程访问完全支持驱动器号和通用命名约定（UNC）名称，所以，大多数商用应用程序和自定义应用程序不必进行修改即可使用。

运行“路由和远程访问”的服务器可提供两种不同类型的远程访问连接。

1．虚拟专用网络

虚拟专用网络（VPN）可以跨专用网络或公用网络（如 Internet）创建安全的点对点连接。VPN 客户端使用基于 TCP/IP 的特殊协议（称为隧道协议）对 VPN 服务器上的虚拟端口进行虚拟呼叫。虚拟专用网络的最佳示例是与连接到 Internet 的远程访问服务器建立 VPN 连接的 VPN 客户端。远程访问服务器应答虚拟呼叫，对呼叫者进行身份验证，并在 VPN 客户端与公司网络之间传输数据。

与拨号网络相反，VPN 始终是通过公用网络（如 Internet）在 VPN 客户端与 VPN 服务器之间建立的逻辑间接连接，如图 7-1 所示。为了确保隐私安全，必须对通过该连接发送的数据进行加密。

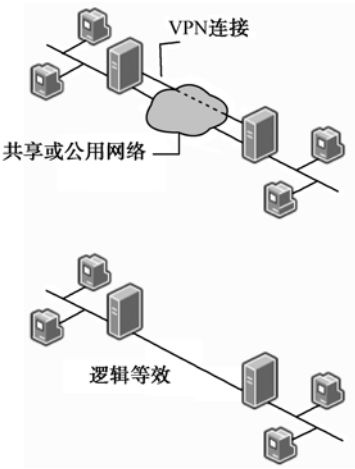

图 7-1　VPN 示意图

2．拨号网络

在拨号网络中，远程访问客户端使用电信提供商的服务（如模拟电话和 ISDN）与远程访问服务器上的物理端口建立非永久的拨号连接。拨号网络的最佳示例是拨打远程访问服务器的一个端口的电话号码的拨号网络客户端。

基于模拟电话或 ISDN 的拨号网络是拨号网络客户端与拨号网络服务器之间的直接物理连接。可以对通过该连接发送的数据进行加密，但并非必须。

虚拟专用网络和拨号网络相比，虚拟专用网络只消耗流量费，不需要拨号，没有电话费，因此费用低廉，所以可以使用 VPN 解决案例中的问题。

7.2.3　相关知识

虚拟专用网络（VPN）是跨专用网络或公用网络（如 Internet）的点对点连接。VPN 客户端使用基于 TCP/IP 的特殊协议（称为隧道协议）对 VPN 服务器上的虚拟端口进行虚拟呼叫。在典型的 VPN 部署中，客户端通过 Internet 启动与远程访问服务器的虚拟点对点连接。远程访问服务器应答呼叫，对呼叫方进行身份验证，并在 VPN 客户端与组织的专用网络之间传输数据。

为了模拟点对点链路，使用标头来封装数据。标头提供路由信息，使数据可以通过共享网络或公用网络到达其终结点。为了模拟专用链路，可对所发送的数据进行加密，以保证机密性。如果没有加密密钥，将难以辨识在共享网络或公用网络上截获的数据包。封装并加密专用数据的链路称为 VPN 连接。

有以下两种类型的 VPN 连接。

1．远程访问 VPN

远程访问 VPN 连接使在家中或路上工作的用户可以使用公用网络（如 Internet）提供的基础结构来访问专用网络上的服务器。从用户的角度来看，VPN 是计算机（VPN 客户端）与组织的服务器之间的点对点连接，与共享网络或公用网络确切的基础结构是不相关的，因为 VPN 是以逻辑形式出现的，仿佛数据通过专用链路发送一样，如图 7-2 所示。本章讨论的主要是远程访问 VPN。

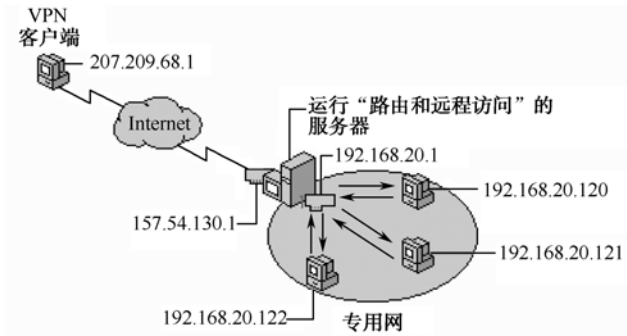

图 7-2　VPN 原理图

2．站点间 VPN

站点间 VPN 连接（也称为路由器间 VPN 连接）使组织可以在各个独立的办公室之间或与其他组织之间通过公用网络建立路由的连接，同时帮助保证通信的安全。跨 Internet 的路由 VPN 连接在逻辑上作为专用广域网（WAN）链路使用。通过 Internet 连接网络时（如图 7-3 所示），路由器将通过 VPN 连接将数据包转发到其他路由器。对于路由器，VPN 连接作为数据链路层链路使用。

站点间 VPN 连接用于连接专用网络的两个部分。VPN 服务器提供与 VPN 服务器连接到的网络的路由连接。呼叫路由器（VPN 客户端）向应答路由器（VPN 服务器）进行自我身份验证。为了进行相互身份验证，应答路由器也向呼叫路由器进行自我身份验证。在站点间 VPN 连接中，从任意一个路由器通过 VPN 连接发送的数据包通常不是源自路由器。

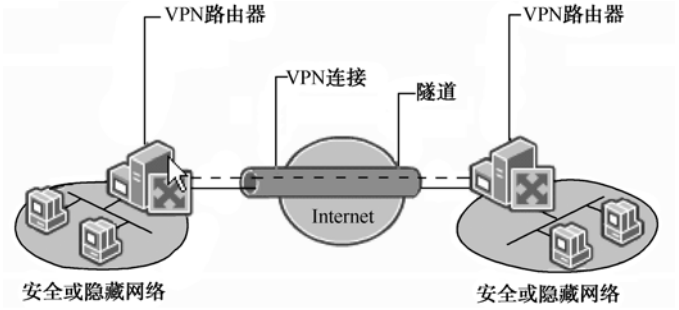

图 7-3　站点间的 VPN

7.3　案例实施过程

本案例架设一个基本的 VPN 服务器，在客户端进行 VPN 连接，主要的步骤如下。

（1）架设 VPN 服务器。

（2）给予用户远程访问的权限。

（3）在 VPN 客户端建立 VPN 连接。

实施案例的网络拓扑结构如图 7-4 所示，图中 VPN 服务器有两块网卡，分别连接企业专用网和 Internet，地址分别为 10.1.1.1 和 1.1.1.1，专用网内服务器地址为 10.1.1.100，远程访问客户端地址为 1.1.1.2。这里的地址是在虚拟机中设置的，真实配置时要根据实际情况做相应改变。

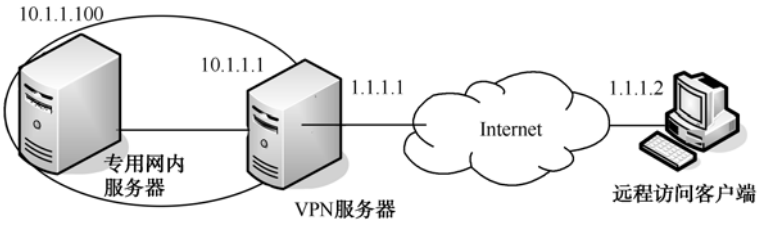

图 7-4　网络拓扑结构

7.3.1　任务 1：架设 VPN 服务器

架设 VPN 服务器包括两个主要步骤。

1．安装路由和远程访问服务

以下步骤在图 7-4 中的“VPN 服务器”中配置。

（1）在“服务器管理器”窗口的“角色摘要”下，单击“添加角色”。在“添加角色向导”中，单击“下一步”按钮。在服务器“角色”列表中，选择“网络策略和访问服务”，如图 7-5 所示，单击两次“下一步”按钮。

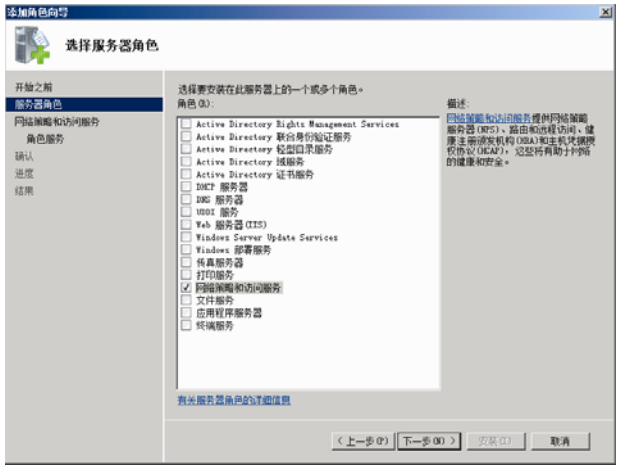

图 7-5　添加角色

（2）在“角色服务”列表中，选择“路由和远程访问服务”以选择所有角色服务，也可以单独选择某一项服务器角色，如图 7-6 所示。

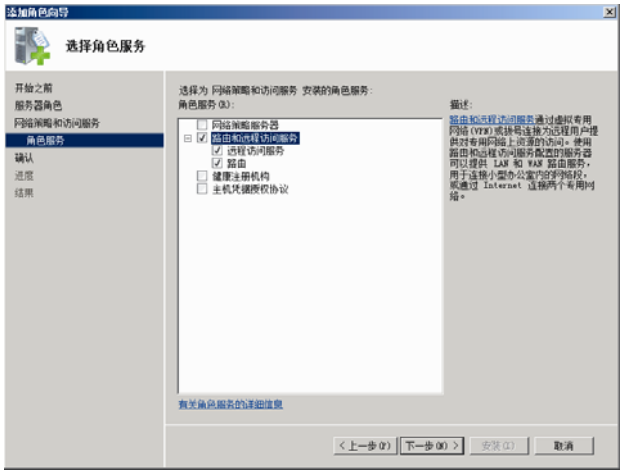

图 7-6　选择“路由和远程访问服务”

（3）继续执行“添加角色向导”中的步骤，以完成安装。

注意：

完成安装之后，安装的“路由和远程访问服务”处于禁用状态。若要启用并配置远程访问服务器，必须以 Administrators 组成员的身份登录。

安装了“路由和远程访问”服务之后，需要启用该服务，才能为您的服务器配置路由和远程访问。

2．启用路由和远程访问服务

以下步骤在图 7-4 中的“VPN 服务器”中配置。

（1）如果此服务器是 Active Directory 域的成员，而您又不是域管理员，则需要要求您的域管理员将此服务器的计算机账户添加到此服务器所属的域中的 RAS and IAS Servers 安全组。域管理员可以使用“Active Directory 用户和计算机”或使用 netsh ras add registeredserver

命令将该计算机账户添加到 RAS and IAS Servers 安全组。如果此服务器使用本地身份验证或针对 RADIUS 服务器进行身份验证，则跳过此步骤。

（2）单击“开始”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”控制台。在控制台树中，右击要启用的服务器，然后单击“配置并启用路由和远程访问”，如图 7-7 所示。

（3）在弹出的“路由和远程访问服务器安装向导”对话框中单击“下一步”按钮，弹出如图 7-8 所示的“配置”对话框，选中“远程访问（拨号或 VPN）”，单击“下一步”按钮。

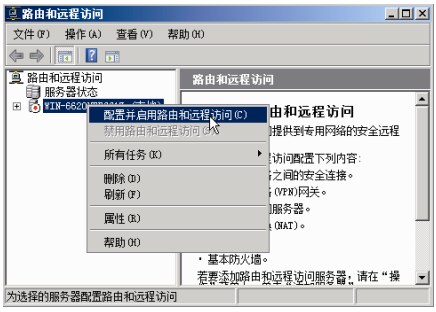

图 7-7　配置并启用路由和远程访问

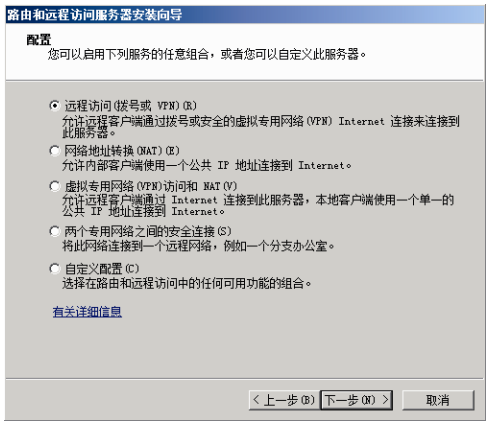

图 7-8　选择远程访问

（4）在“远程访问”对话框中勾选“VPN”，单击“下一步”按钮，如图 7-9 所示。

（5）在“VPN 连接”对话框中选中连接到 Internet 的网络连接口，本例中是“本地连接 2”。在对话框中如果勾选了“通过设置静态数据包筛选器来对选择的接口进行保护”，那么在这台计算机上将不能访问 Internet，只能接受 VPN 客户的访问，单击“下一步”按钮，如图 7-10 所示。

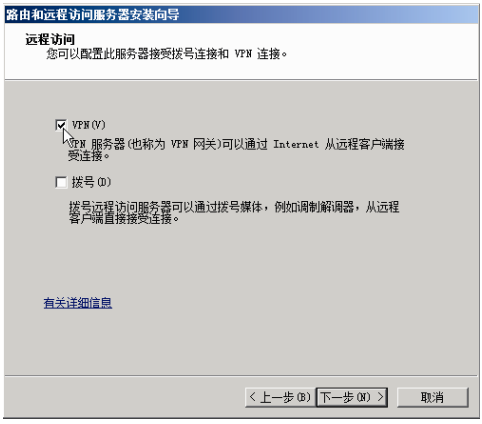

图 7-9　选择“VPN”

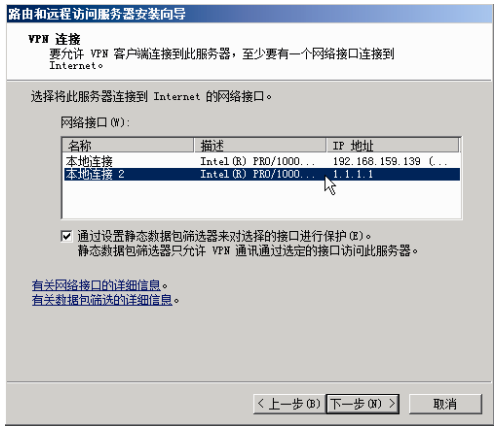

图 7-10　选择 VPN 连接的网络接口

（6）在“IP 地址分配”对话框中选择如何对远程用户分配 IP 地址。

如果你的公司网络中有 DHCP 服务器，就选中“自动”，这时远程用户将能够从 DHCP 服务器中获取 IP 地址。

如果你的公司网络中没有 DHCP 服务器，就选中“来自一个指定的地址范围”，这时远程用户将能够从你在下个步骤中指定的 IP 地址中获取 IP 地址。

本例选中“来自一个指定的地址范围”，单击“下一步”按钮，如图 7-11 所示。

（7）在“地址范围分配”对话框中单击“新建”按钮，在“新建 IPv4 地址范围”对话框中输入 IP 地址范围。这个地址范围就是上一步中说的“指定的地址范围”。要注意的是，指定的地址范围必须与专用网的地址在同一个网段。单击“下一步”按钮，如图 7-12 所示。

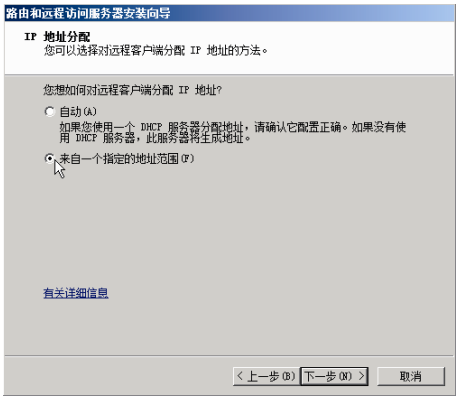

图 7-11　选择指定 IP 地址

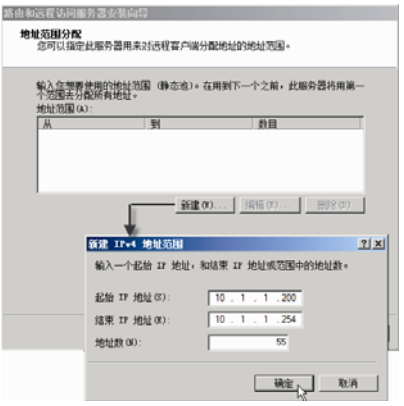

图 7-12　添加指定的 IP 地址

（8）在“管理多个远程访问服务器”对话框中选择由谁来验证远程用户的身份。如果由本服务器验证，选择“否，使用路由和远程访问来对连接请求进行身份验证”，如果使用 RADIUS 服务器进行远程用户身份验证，就选中“是，设置此服务器与 RADIUS 服务器一起工作”。RADIUS 服务器是专门用来验证用户身份的服务器。如图 7-13 所示，单击“下一步”按钮后，单击“完成”按钮。

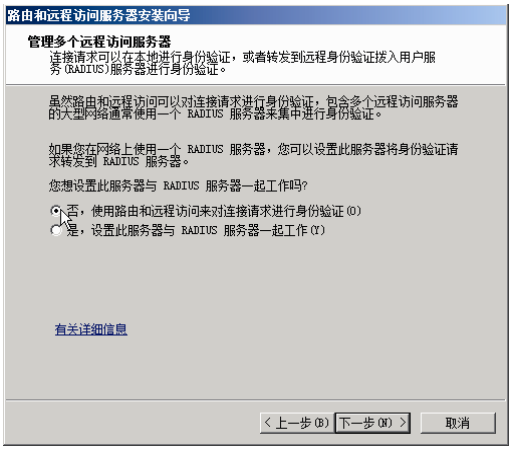

图 7-13　选择由谁来进行身份验证

7.3.2　任务 2：给予用户远程访问的权限

默认情况下，用户没有远程访问的权限，必须赋予用户远程访问的权限后用户才能远程访问。

（1）找到要赋予远程访问权限的用户。

在域控制器中，单击“开始”→“管理工具”→“Active Directory 用户和计算机”，找到要赋予远程访问权限的用户。

在非域控制器中，单击“开始”→“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”→“用户”，找到要赋予远程访问权限的用户。

本例在非域控制器中配置，即在图中的 VPN 服务器中进行配置。

（2）右击要赋予远程访问权限的用户，如本例中的用户 zhangfei，单击“属性”，在“属性”对话框中单击“拨入”选项卡，选中“网络访问权限”中的“允许访问”，如图 7-14 所示，单击“确定”按钮。

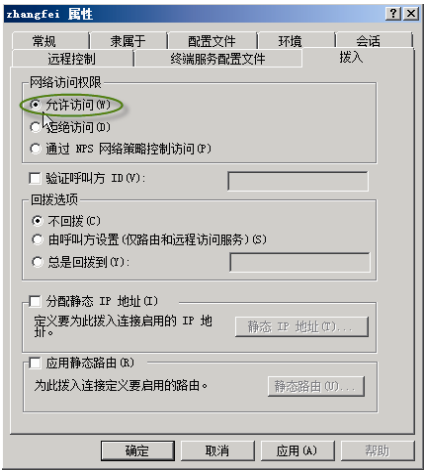

图 7-14　赋予用户远程访问权限

7.3.3　任务 3：从 VPN 客户端建立 VPN 连接

以下步骤在图 7-4 中的“远程访问客户端”中配置。

下面以 Windows 7 系统为例说明如何建立客户端 VPN 连接。

（1）单击“开始”→“控制面板”→“查看网络状态和任务”，打开“网络和共享中心”，单击“设置新的连接或网络”，如图 7-15 所示。

图 7-15　打开网络连接

（2）单击“连接到工作区”，如图 7-16 所示。单击“下一步”按钮。

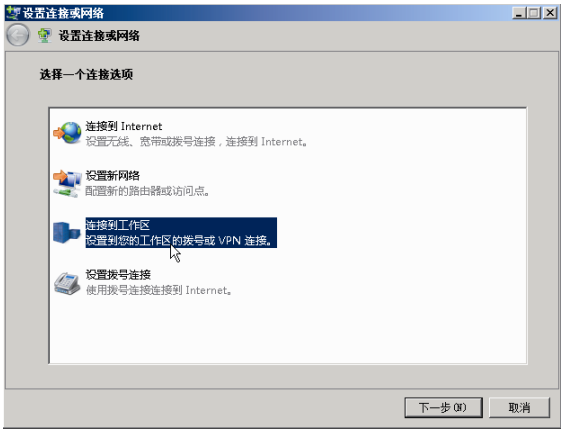

图 7-16　选择网络连接类型

（3）在图 7-17 中单击“使用我的 Internet 链接（VPN）”，单击“下一步”按钮。

图 7-17　选择 VPN 连接

（4）在图 7-18 中单击“我将稍后设置 Internet 连接”。

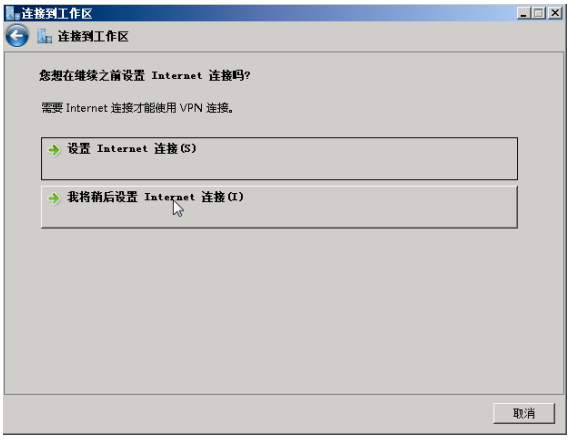

图 7-18　暂不设置 Internet 连接

（5）在图 7-19 中输入“Internet 地址”为 1.1.1.1，也就是 VPN 服务器连接 Internet 的网络适配器的地址，单击“下一步”按钮。

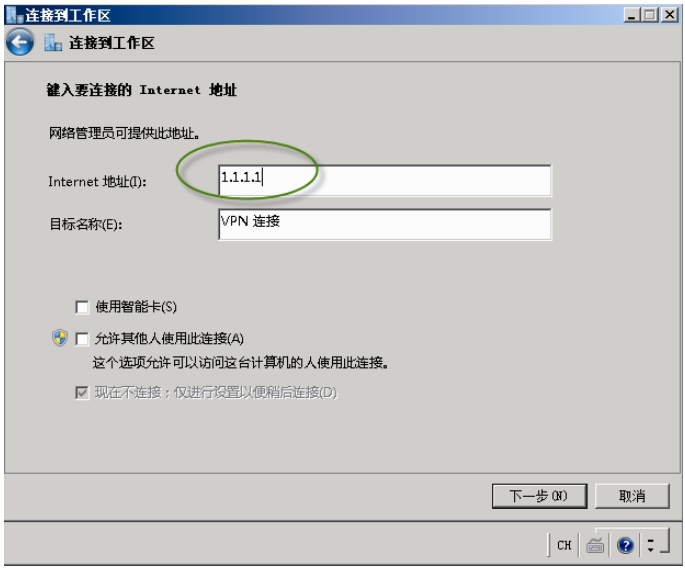

图 7-19　输入 VPN 服务器的地址

（6）在图 7-20 中输入有权限进行 VPN 连接的用户名和密码，单击“创建”按钮，再单击“关闭”按钮。

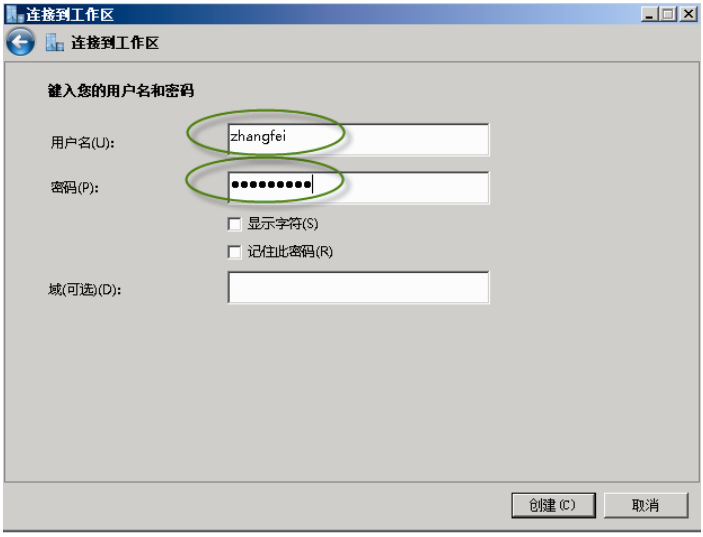

图 7-20　输入有权限进行 VPN 连接的用户

（7）在“网络和共享中心”中单击“连接到网络”，在弹出的对话框中单击“连接”按钮，如图 7-21 所示。

（8）在图 7-22 中输入有权限进行 VPN 连接的用户名和密码，单击“连接”按钮。

图 7-21　连接 VPN

图 7-22　输入用户名和密码

（9）VPN 连接后，在“网络和共享中心”中将显示有 VPN 的网络连接，如图 7-23 所示。

图 7-23　VPN 连接后的情况

（10）这时的计算机将可以访问公司的网络了。比如，可以访问图 7-4 中“专用网内服务器”中的共享文件夹。方法是单击“开始”→“运行”，输入“\\10.1.1.100”后按回车键（10.1.1.100 是“专用网内服务器”的 IP 地址），就可以看到“专用网内服务器”内的共享文件夹了，如图 7-24 所示。

图 7-24　使用 VPN 能在公网中访问公司的网络资源

7.4　知识能力拓展 1：建立 L2TP VPN

前面章节建立的 VPN 连接类型为 PPTP，除了 PPTP VPN 外，还有两种类型的 VPN，即 L2TP VPN 和 SSTP VPN。

点对点隧道协议（PPTP）是由包括微软和 3COM 等公司组成的 PPTP 论坛开发的一种点对点隧道协议，基于拨号使用的 PPP 协议使用 PAP 或 CHAP 之类的加密算法，或者使用 Microsoft 的点对点加密算法 MPPE。它通过跨越基于 TCP/IP 的数据网络创建 VPN，实现了从远程客户端到专用企业服务器之间数据的安全传输。PPTP 支持通过公共网络（如 Internet）建立按需的、多协议的虚拟专用网络。PPTP 允许加密 IP 通信，然后在要跨越公司 IP 网络或公共 IP 网络（如 Internet）发送的 IP 头中对其进行封装。

L2TP 第 2 层隧道协议（L2TP）是一种工业标准的 Internet 隧道协议，它可以为跨越面向数据包的媒体发送点到点协议（PPP）框架提供封装。PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加附加包头用于数据在因特网上的传输。PPTP 只能在两端点间建立单一隧道。L2TP 支持在两端点间使用多隧道，用户可以针对不同的服务质量创建不同的隧道。L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。

安全套接字隧道协议（SSTP）是一种新形式的虚拟专用网络（VPN）隧道，具有允许通信通过阻止 PPTP 和 L2TP/IPSec 通信的防火墙的功能。SSTP 提供了一种机制，可以封装通过 HTTPS 协议的 SSL 通道传输的 PPP 通信。使用 PPP 可以支持强大的身份验证方法，如 EAP-TLS。使用 HTTPS 意味着通信将流经 TCP 端口 443（常用于 Web 访问的端口）。安全套接字层（SSL）通过增强的密钥协商、加密和完整性检查，提供传输级别的安全性。

下面分别介绍 L2TP VPN 和 SSTP VPN。

7.4.1　建立 L2TP IPSec VPN 连接

要建立 L2TP IPSec VPN 连接，VPN 服务器和客户端都需要申请和安装身份验证证书和根 CA 证书，因此需要建立证书服务器。

本书只介绍向独立 CA 申请的步骤，向企业 CA 申请的步骤与向独立 CA 申请的步骤大同小异。

如图 7-25 所示是使用 IPSec 建立 L2TP VPN 连接的网络拓扑。CA 服务器提供独立 CA 服务，并且启用了 SSL。

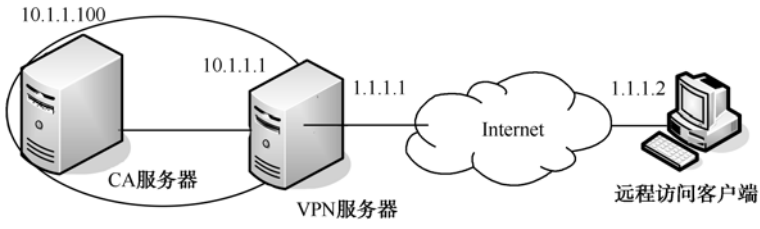

图 7-25　L2TP IPSec VPN 拓扑图

VPN 服务器和 VPN 客户端都需要申请证书，下面分别说明。

1．VPN 服务器申请服务器根 CA 证书

VPN 服务器必须信任证书服务器，因此必须申请并下载根 CA 证书。

（1）打开浏览器，在地址栏输入“https://CA 服务器地址或域名/certsrv”，输入域管理员的用户名和密码，如果弹出如图 7-26 所示的对话框，则单击“添加”按钮，把 CA 服务器添加到信任站点中。

单击“下载 CA 证书、证书链或 CRL”，如图 7-27 所示。

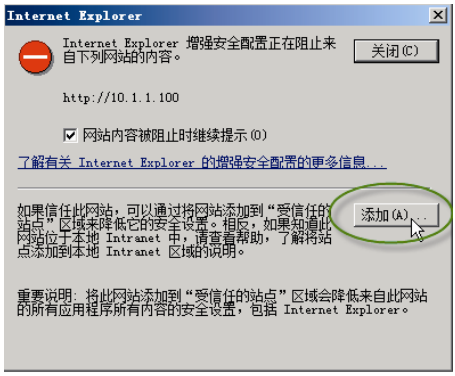

图 7-26　将 CA 服务器添加到信任站点中

图 7-27　下载 CA 证书、证书链或 CRL

（2）在图 7-28 中单击“下载 CA 证书”，在“文件下载–安全警告”中单击“保存”按钮，把 CA 证书保存到计算机中的适当位置。

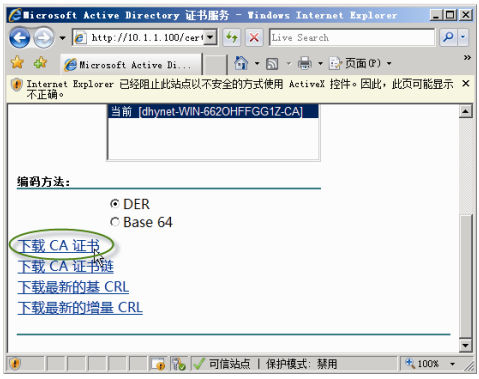

图 7-28　下载 CA 证书

（3）单击“开始”→“运行”，输入“mmc”，然后单击“确定”按钮。

（4）在“文件”菜单上单击“添加/删除管理单元”。

（5）在“可用的管理单元”列表中单击“证书”，然后单击“添加”按钮。

（6）在“证书管理单元”对话框中单击“计算机账户”，然后单击“下一步”按钮。

（7）使“本地”计算机选项处于选中状态，然后单击“完成”按钮。

（8）在“可用的管理单元”列表中单击“证书”，然后单击“添加”按钮。

（9）在“证书管理单元”对话框中单击“我的用户账户”，然后单击“完成”按钮。

（10）在“添加或删除管理单元”对话框中单击“确定”按钮。

（11）在图 7-29 中单击“证书（本地计算机）”→“受信任的根证书颁发机构”，右击“证书”，单击“所有任务”→“导入”，打开“证书导入向导”，单击“下一步”按钮。

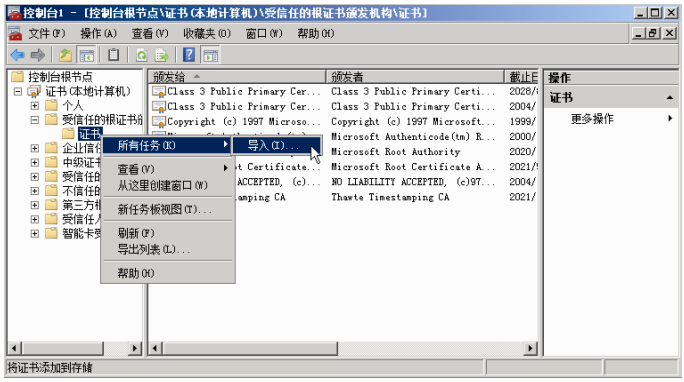

图 7-29　把证书导入到“证书（本地计算机）”中

（12）在图 7-30 中的“文件名”文本框中输入在步骤（2）中保存的 CA 证书的路径和文件名，或者单击“浏览”，找到在步骤（2）中保存的 CA 证书，单击两次“下一步”按钮，再单击“完成”按钮，完成 CA 证书的导入。图 7-31 是证书导入后的情况。

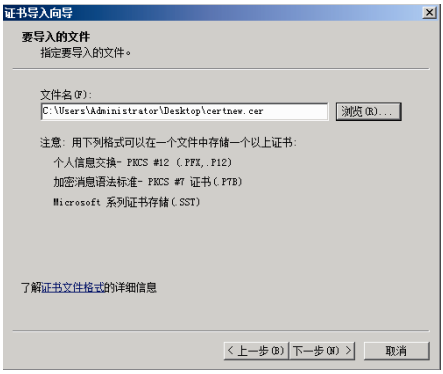

图 7-30　找到要导入的证书

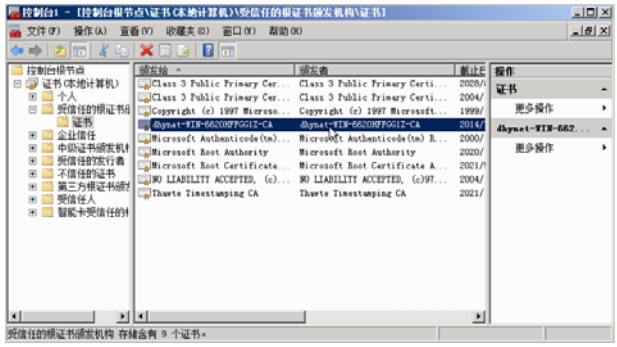

图 7-31　证书导入后的情况

2．VPN 服务器申请身份验证证书

（1）在 IE 浏览器中输入地址“https://CA 的 IP 地址或域名”，输入连接到 CA 服务器的用户名和密码（如域管理员），单击“申请证书”→“高级证书申请”→“创建并向此 CA 提交一个申请”，如图 7-32 所示。

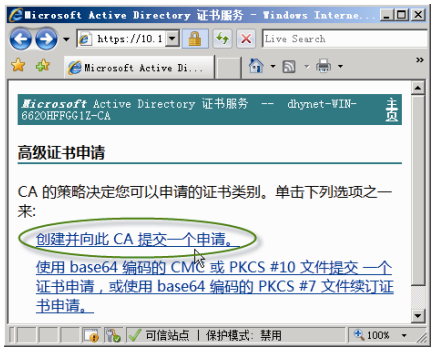

图 7-32　申请证书

（2）在图 7-33 中输入相应信息，在“姓名”处输入 VPN 服务器的域名或者 IP 地址，在“需要的证书类型”中选择“服务器身份验证证书”，单击“提交”。

（3）图 7-34 显示的是提交成功的画面，等待管理员颁发证书。

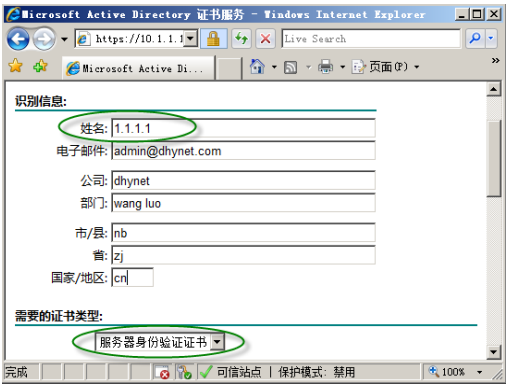

图 7-33　输入证书信息

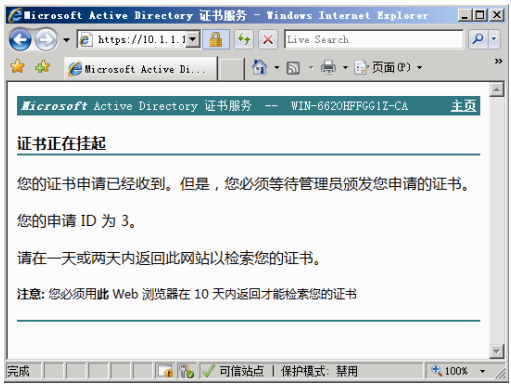

图 7-34　证书提交成功

（4）在证书服务器中颁发证书。单击“开始”→“管理工具”→“证书颁发机构”，颁发证书，如图 7-35 所示。

（5）在 VPN 服务器中，查看所申请的证书并安装。在 IE 浏览器中输入地址“https://CA 的 IP 地址或域名”，单击“查看挂起的证书申请状态”，如图 7-36 所示。

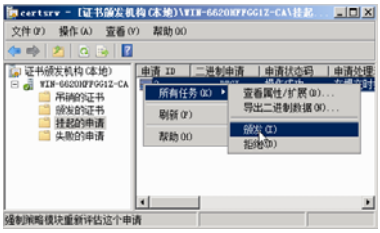

图 7-35　颁发证书

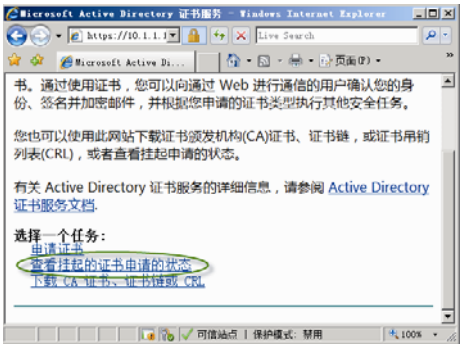

图 7-36　查看挂起的证书申请状态

（6）在图 7-37 中，单击“服务器身份验证证书”。

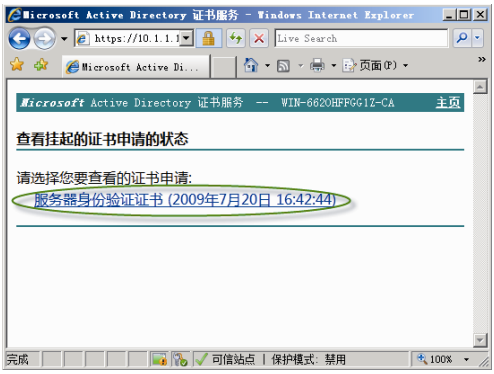

图 7-37　颁发后的证书

（7）在图 7-38 中，单击“安装此证书”。证书安装完成后，关闭浏览器。

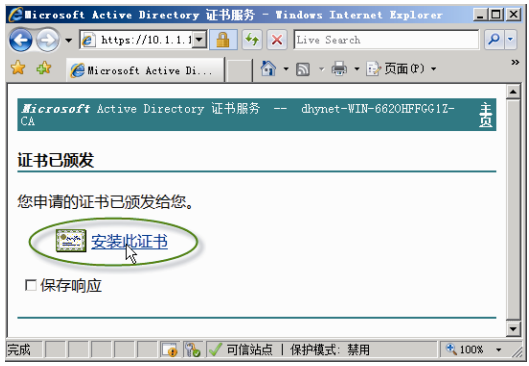

图 7-38　安装证书

说明：以上步骤申请并安装了证书。这个证书被安装在“证书-当前用户”下面，还需要把这个证书导出，然后导入到“证书（本地计算机）”下面。下面的步骤说明了证书导出和导入的操作步骤。

（8）单击“开始”→“运行”，输入“mmc”按回车键，打开控制台。在控制台中单击“文件”→“添加/删除管理单元”，添加“证书-当前用户”和“证书（本地计算机）”两个管理单元。在证书控制台中，单击“证书-当前用户”→“个人”→“证书”，在右边窗格中右击前面申请的证书，单击“所有任务”→“导出”，如图 7-39 所示。然后按照提示使用默认操作把证书导出到计算机的磁盘中。

（9）在图 7-40 中单击“证书（本地计算机）”→“个人”，右击“证书”，单击“所有任务”→“导入”，打开“证书导入向导”，按照提示把步骤（10）中导出的证书导入。

图 7-39　导出证书

图 7-40　导入到“证书（本地计算机）”

3．VPN 客户端申请根 CA 证书和客户端身份验证证书

VPN 客户端申请根 CA 证书和客户端身份验证证书的方法与上述 VPN 服务器申请服务器身份验证证书的过程基本一样，需要注意的不一样的地方如下。

（1）要考虑 VPN 客户端如何和 CA 连接的问题。因为客户端一般位于 Internet 中，CA 一般位于内网（公司专用网）中，通常情况下 VPN 客户端无法访问 CA。解决的办法有两种。

- 如果是公司的笔记本电脑，可以事先申请并安装，再出差。
- 先用 PPTP VPN 的方式连接，然后再申请。

本例使用后一种方法，即先连接上 PPTP VPN，然后再申请。

（2）申请的证书模板是“用户”，如图 7-41 所示。

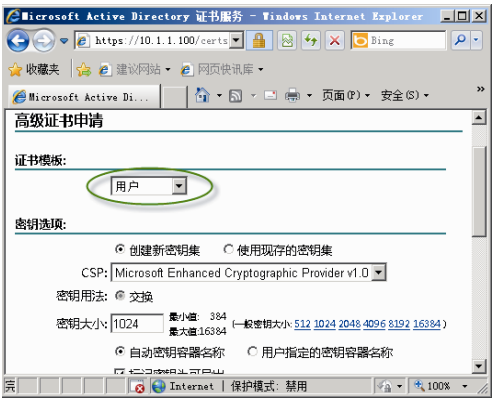

图 7-41　用户申请的证书模板

7.4.2　配置 VPN 客户端使用 L2TP IPSec VPN 并连接

在 VPN 客户端打开网络连接，如果虚拟专用网络接口已经连接，先要断开连接，然后右击虚拟专用网络接口，单击“属性”，在弹出的对话框中选择“安全”选项卡，选择“VPN 类型”为“使用 IPsec 的第 2 层隧道协议（L2TP/IPSec）”，单击“确定”按钮，如图 7-42 所示。然后右击虚拟专用网络接口，单击“连接”，连接成功，这时使用的即是 L2TP 连接。

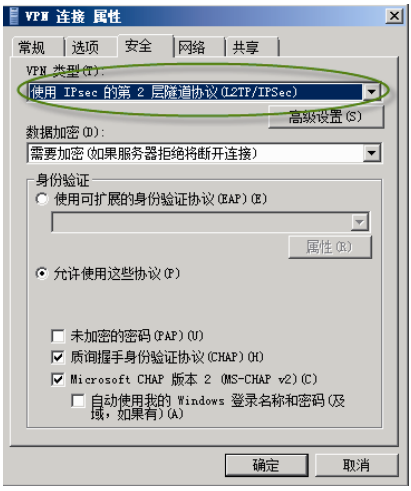

图 7-42　配置 VPN 的连接类型为 L2TP/IPSec

7.4.3　使用预共享密钥进行 L2TP VPN 连接

使用预共享密钥进行 L2TP VPN 连接比较简单。在配置好 PPTP VPN 的服务器中，单击“开始”→“管理工具”→“路由和远程访问”，右击服务器名，选择“属性”，在打开的对

话框中选择“安全”选项卡，勾选“允许 L2TP 连接使用自定义 IPsec 策略”，并设置“预共享的密钥”，单击“确定”按钮，如图 7-43 所示。

在 VPN 客户端（以 Windows 7 操作系统为例）打开网络连接，如果虚拟专用网络接口已经连接，先要断开连接，然后右击虚拟专用网络接口，单击“属性”，在打开的对话框中选择“安全”选项卡，选择“VPN 类型”为“使用 IPsec 第 2 层隧道协议（L2TP/IPSec）”，然后单击“高级设置”按钮，在弹出的对话框中勾选“使用预共享的密钥作身份验证”，输入与 VPN 服务器中相同的密钥，如图 7-44 所示。单击两次“确定”按钮。

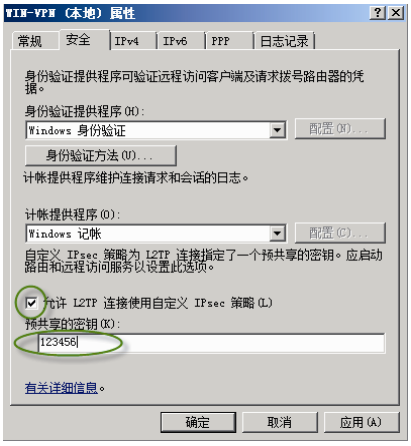

图 7-43　在服务器端设置预共享密钥

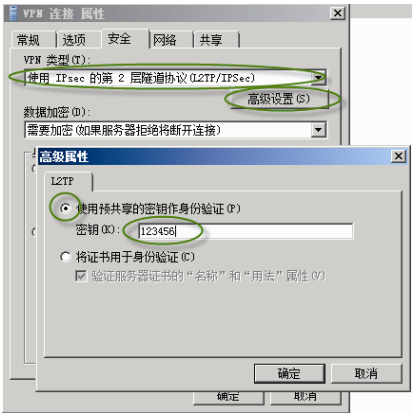

图 7-44　客户端设置预共享密钥

7.5　知识能力拓展 2：建立 SSTP VPN

SSTP 是微软提供的新一代的虚拟专用网（VPN）技术，它的全称是安全套接层隧道协议（Secure Socket Tunneling Protocol，SSTP）。与 PPTP L2TP OVER IPSec 一样，也是微软所提供的 VPN 技术。它在拥有最大弹性发挥的同时，又确保了信息安全。

目前，支持 SSTP 技术的仅限于如下 OS：Windows Vista SP1、Windows 7 及 Windows Server 2008。通使用此项新技术，可以让防火墙管理员能更容易地配置策略，以使 SSTP 流量通过其防火墙。它提供了一种机制，将 PPP 数据包封装在 HTTPS 的 SSL 通信中，从而使 PPP 支持更加安全的身份验方法，如 EAP-TLS 等。

新的 SSTP 协议的支持，并没有完全否决 PPTP 及 L2TP OVER IPSec 在微软产品所组成的解决方案中的作用，当企业使用基于 Windows 平台的 VPN 解决方案时，这种协议仍是最常被用来解决或是提升企业网络安全性的。但两者的数据包通过防火墙、NAT、Web Proxy 时却都有可能发生一些连接方面的问题。

PPTP 数据包通过防火墙时，防火墙需被设定成同时允许 TCP 连接及 GRE 封装的数据通过，但大部分 ISP 都会阻止这种封包，从而造成连接的问题；而当你的机器位于 NAT 之中时，NAT 也必须被设定成能转发 GRE 协议封装的数据包。否则就会造成只能建立 PPTP 的 TCP 连接，而无法接收 GRE 协议封装的数据包；Web Proxy 是不支持 PPTP 协议的。

L2TP OVER IPSec 的情况和此类似，需要在防火墙上允许 IKE 数据和 ESP 封装的数据同时通过，否则也会出现连接问题，而且 Web Proxy 也是不支持 L2TP OVER IPSec 协议的。

SSTP 解决了 PPTP 和 L2TP 的上述不足。

SSTP VPN 的安装和配置与 L2TP VPN 大部分一样，下面重点叙述不一样的地方。

1．VPN 服务器端

在 VPN 服务器端要配置 VPN 服务器能发布 CA 的证书吊销列表 CRL，因为客户端在访问 VPN 服务器时，要查询 CRL。这就要求增加下面两处配置。

一是在启用路由和远程访问时，单击“开始”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”控制台。在控制台树中，右击要启用的服务器，然后单击“配置并启用路由和远程访问”。在弹出的“路由和远程访问服务器安装向导”对话框中单击“下一步”按钮，弹出如图 7-45 所示的“配置”对话框，选中“虚拟专用网络(VPN)访问和 NAT”。前面叙述的几种 VPN 都是选中“远程访问（拨号或 VPN）”选项。

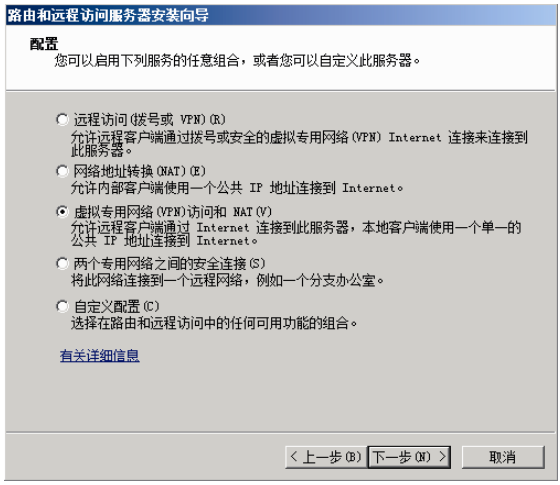

图 7-45　配置 VPN 和 NAT

二是在路由和远程访问服务器安装完成后，要配置 VPN 服务器能发布 CA 的网站。步骤如下。

（1）在“路由和远程访问”控制台中，依次展开“VPN 服务器”→“IPv4”→“NAT”，在右侧窗格中右击连接 Internet 的网络接口（本例是“本地连接 2”），单击“属性”，如图 7-46 所示。

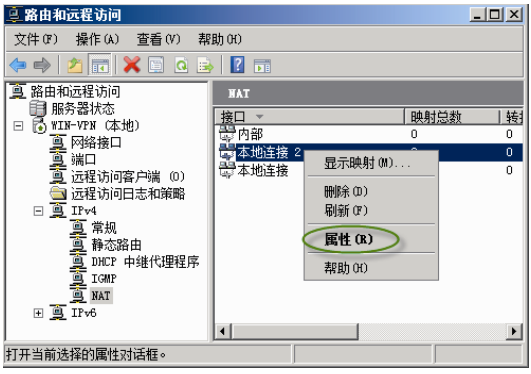

图 7-46　打开网络适配器属性

（2）在“本地连接 2 属性”对话框中，单击“服务和端口”选项卡，勾选“Web 服务器（HTTP）”选项，如图 7-47 所示。

（3）在弹出的“编辑服务”对话框中的“专用地址”文本框中输入 CA 服务器的地址，如图 7-48 所示。单击两次“确定”按钮，即完成了发布 CA 的证书吊销列表的功能。

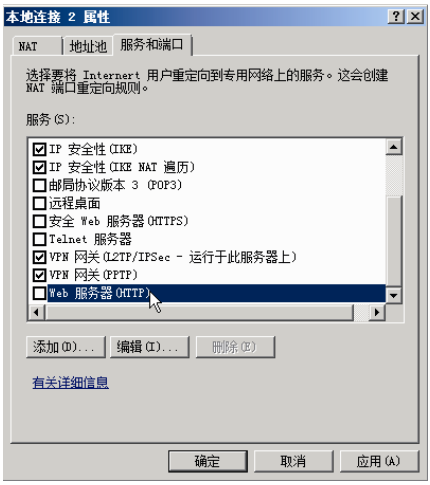

图 7-47　设置网络适配器属性

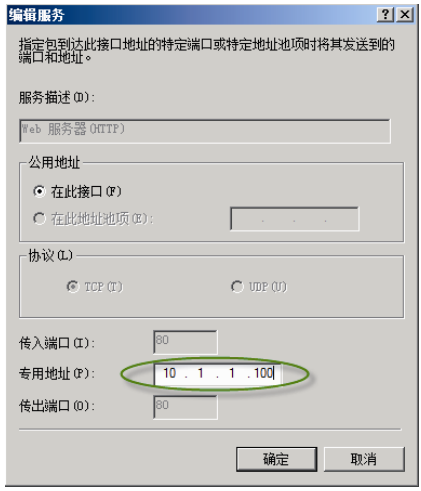

图 7-48　设置内部地址

服务器端申请的服务器身份验证证书的名称必须与服务器的计算机名/完全合格的域名一致。如图 7-49 所示，“姓名”文本框中输入的是 VPN 服务器的域名。

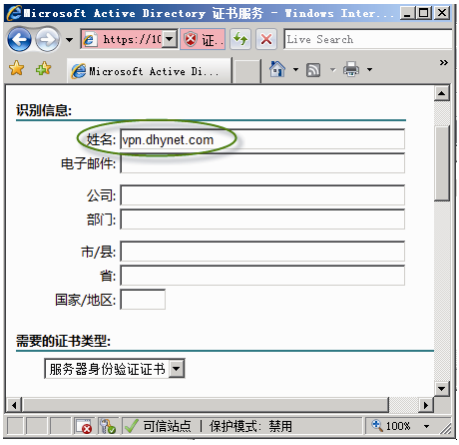

图 7-49　姓名必须与计算机名一致

2．VPN 客户端

SSTP VPN 的客户端与 L2TP VPN 的客户端有 3 处不同。

（1）不需要安装客户端身份验证证书，但根 CA 证书还是要安装的。

（2）在 VPN 连接的“VPN 类型”中要选择“安全套接字隧道协议（SSTP）”，如图 7-50 所示。

（3）在 VPN 连接的目的主机中要输入 VPN 服务器的完全合格的域名/计算机名，如图 7-51 所示。

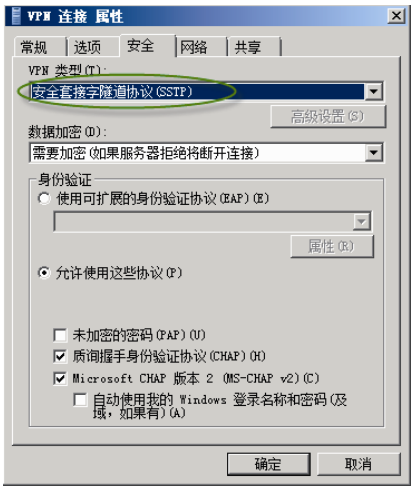

图 7-50　设置 VPN 类型

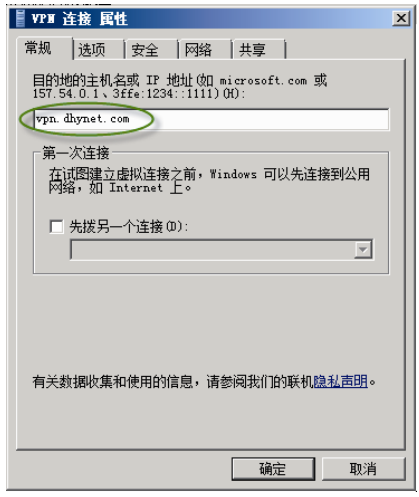

图 7-51 设置连接名

7.6　项目完成结论

配置 VPN 服务器需要注意，安装路由和远程访问服务器时，选择连接到 Internet 的网络接口时要小心，不要错选为连接内网的网络接口。分配给 VPN 客户端的 IP 地址要与工作场所使用的 IP 的网络地址相同，即在同一个网段，否则即使能够连接到 VPN 服务器，也不能连接到工作场所的网络。

7.7　练习案例

DHYNET 公司为员工配置了笔记本电脑，并且安装了 Windows 7 操作系统。这些员工经常出差，在出差时需要访问公司的安全 Web 服务器（HTTPS），请你为 DHYNET 公司提供解决方案。

7.8　课后习题

1．公司为什么要使用 VPN 服务？
2．VPN 服务有哪些类型？各有什么特点？
3．在各种 VPN 服务的配置中，有什么相同的地方？有什么不同的地方？
4．简述各种 VPN 类型的 VPN 配置过程。
5．在完成本章的各个练习的过程中，你遇到了哪些问题？是怎么解决的？

项目 8　终端服务的安装、配置与管理

终端服务在我们的日常管理与维护过程中发挥着非常重要的作用。使用终端服务，员工无论是在办公室、在家，还是在旅途中，都可以通过 Internet 远程访问终端服务器，方便而有效地部署和维护软件。通过 Windows Server 2008 中的“终端服务”服务器角色所提供的技术，用户可以访问安装在终端服务器上的基于 Windows 的程序或访问完整的 Windows 桌面，节省了大量成本且显著提高了工作效率。终端服务提供了在 Windows Server 上承载多个并发客户端会话的能力。基于 Windows 的标准应用程序无须做任何修改便可在终端服务器上运行，而且可以使用所有标准的 Windows Server 管理基础结构和技术来管理客户端桌面系统。通过这种方式，企业能够从当今 Windows 操作系统环境提供的丰富应用程序和工具选择中做出适合自己需要的选择。

知识点、技能点

- 了解终端服务的原理及作用
- 掌握终端服务器的安装
- 掌握终端服务的部署
- 熟悉应用程序的连接
- 熟悉 Web 应用程序的访问
- 熟悉 Windows 系统资源管理器的使用

8.1　引例：为什么要使用终端服务（WHY）

终端服务在我们的日常管理与维护过程中发挥着非常重要的作用，利用终端服务可以进行远程管理与维护，提供远程访问应用程序等功能，节省了大量成本且显著提高了工作效率。

使用终端服务，员工无论是在办公室、在家，还是在旅途中，几乎在任何地点，都可以连接到终端服务器，运行基于视窗程序或完全视窗桌面的服务器，使用该服务器上的网络资源。

使用终端服务，用户可以在企业网络内部或通过 Internet 访问终端服务器。各种基于 Windows 的标准应用程序无须做任何修改便可在终端服务器上运行，而且可以使用所有标准的 Windows Server 管理基础结构和技术来管理客户端桌面系统。通过使用终端服务，企业能够从当今 Windows 操作系统环境提供的丰富应用程序和工具选择中做出适合自己需要的灵活选择。

因此集中在终端服务器上（而不是在每台设备上）部署程序，可以带来很多益处。例如，可以快速地将基于 Windows 的程序部署到整个企业中的计算设备上，在程序经常需要更新、很少使用或难以管理的情况下，终端服务尤其有用；终端服务可以显著减少访问远程应用程序所需的网络带宽；终端服务有助于提高用户的工作效率，用户可以通过家用计算机、展台、低能耗硬件等设备，以及非 Windows 操作系统访问终端服务器上运行的程序；对于需要访问中心数据存储的分支机构工作人员来说，终端服务可提供更好的程序性能；有时，数据密集型程序没有针对低速连接进行优化的客户-服务器协议；与典型的广域网连接比较，此类通过终端服务连接运行的程序性能会更好。

8.2　案例 1：远程管理你的服务器

8.2.1　工作情景描述

你是 DHYNET 公司的网络管理员。DHYNET 公司有多台服务器和计算机，它们使用了微软公司的软件产品，包括操作系统、办公软件等。你管理着这些服务器。你是一个模范的员工，你可以在 8 小时之内坚守职责，维护服务器，或用计算机处理公司事务，但是在某一天下班时间或者是在你休假的时候，甚至是你正在外地出差时，公司主管通知你管理和维护这些服务器，或用计算机处理公司事务，让它执行各种的程序。你手头只有笔记本电脑，可以通过无线网络远程连接公司网络的服务器或办公室的计算机。又或者你在公司总部工作，总部只有很少的几个网管员，你的企业的数个分支机构的计算机需要统一连接到总部服务器应用特定软件，那么你该如何解决这样的问题呢？

8.2.2　案例分析

只要公司总部网络服务器、分支机构的服务器或办公室的计算机开启了终端服务，那么我们无论在任何地方都可以对办公室的服务器进行控制，继续我们的工作。无论你是在家中，还是在咖啡店、旅馆等场所，或是在旅途中的火车上，你都可以用笔记本电脑通过无线网络，连接自己公司的计算机。远程控制公司的计算机或分支机构的计算机，让它们执行各种工作，甚至你可以在装有 Linux 系统的计算机上，用客户端来控制装有 Windows 系统的计算机。总而言之，有了终端服务，只需要一个客户端程序，就可以让你体验亲身在远程计算机面前进行操作的感觉。

8.2.3　相关知识

1．什么是终端服务

终端服务（Terminal Services，TS）也叫 WBT（Windows-based Terminal，基于 Windows 的终端），这是在 Windows NT 中首先引入的一个服务，存在于 Windows Server 2000/2003/2008 中。终端服务起到的作用就是方便多用户一起操作网络中开启终端服务的服务器，所有用户对同一台服务器进行操作，所有操作和运算都放在该服务器上。终端服务使用 RDP 协议（远程桌面协议）进行客户端连接，使用终端服务的客户可以在远程以图形界面的方式访问服务器，并且可以调用服务器中的应用程序、组件、服务等，和操作本机系统一样。这样的访问方式不仅大大方便了各种各样的用户，而且大大提高了工作效率，能有效地节约企业的成本。

终端服务的工作原理是客户机和服务器通过 TCP/IP 协议和标准的局域网构架进行联系。通过客户端终端，客户机的鼠标、键盘的输入会传递到终端服务器上，再把服务器上的显示传递回客户端，如图 8-1 所示。客户端不需要具有计算能力，至多只需提供一定的缓存能力即可。众多的客户端可以同时登录到服务器上，仿佛同时在服务器上工作一样，它们之间作为不同的会话连接是互相独立的。终端服务所使用的默认端口是 3389 端口。

终端服务可使用户在企业环境中有效地部署和维护软件。可以很容易地从中心位置部署程序。由于将程序安装在终端服务器上，而不是安装在客户端计算机上，因此更容易升级和维护程序。

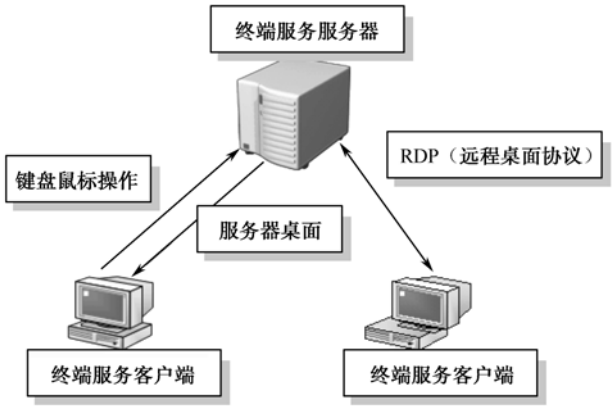

图 8-1　终端服务图解

用户访问终端服务器上的某个程序时，在服务器上执行该程序。只有键盘、鼠标和显示器的信息才通过网络传输。每个用户只能看到自己的会话。服务器操作系统透明地管理会话，与任何其他客户端会话无关。

Windows Server 2008 操作系统的终端服务组件所提供的技术允许用户从几乎任何计算设备访问安装在终端服务器上的基于 Windows 的程序，或访问完整的 Windows 桌面本身。用户可连接到终端服务器来运行程序并使用该服务器上的网络资源。

2．什么是终端服务器

终端服务器是运行终端服务的服务器，它为客户端计算机托管基于 Windows 操作系统的程序或完整的 Windows 桌面。用户可以通过连接客户端计算机到终端服务器来运行程序、保存文件，以及使用该服务器上的网络资源。用户可以使用 Remote Desktop Connection（远程桌面连接，RDC）6.0（RDC 6.0）或更高版本，或 RemoteApp 程序（远程应用程序）访问终端服务器。当服务器处于终端服务器角色的配置中时，就称为终端服务器。

3．终端服务主要应用在哪里

终端服务的目的是为了实现集中化应用程序的访问。终端服务主要应用于以下几种环境中。

1）应用程序的集中部署

在客户-服务器网络体系中，如果客户端需要使用相同的应用程序，如都要使用相同版本的邮件客户端、办公软件等，而客户端部署的操作系统又不尽相同，如 Win 2000、Win XP、Win 7 等，则在网络规模很大时，分别向这些客户端部署相同版本的应用软件是让管理员感到很烦琐的事情，需要大量重复的工作而且需要考虑软件版本的兼容性问题。这时候如果采用终端服务便可以很好地解决这个问题，客户端需要使用的应用软件只需在终端服务器上部署一次即可，无论客户端安装的是什么版本的操作系统，都可以连接到终端服务器使用相同版本的应用软件。

2）分支机构的方便利用

企业分支机构一般没有或者只有很少的专业 IT 管理员，企业如果向各个分支机构委派专门的网络管理员无疑会为企业增加不小的开支。这时候如果分支机构的计算机均采用终端服务的解决方案，统一连接到终端服务器应用特定软件，可以简化 IT 管理员的维护，减少维护成本和复杂程度。

3）任意地点的安全访问

很多时候出差在外的员工需要应用某个特定的应用软件，如公司定制的财务软件等，这时

候员工可以通过手机、笔记本电脑等移动设备，在任意地点连接公司终端服务器进行应用。例如，在 Windows Server 2008 中，用户可以利用终端服务中的 TS Web Access 功能，没必要连接 VPN，仅仅通过 Web 方式即可访问企业终端服务器，并且可以获得良好的用户体验。此外，Windows Server 2008 中的终端服务具有网关功能 TS Gateway，可以裁决用户是否满足连接条件，并且可以确定用户可以连接哪些终端服务器，从而保证了安全性。

4．终端服务都有哪些角色服务

终端服务是由多个子组件（称为“角色服务”）组成的服务器角色。在 Windows Server 2008 中，终端服务由下列角色服务组成。

1）终端服务器

“终端服务器”角色服务使服务器可以托管基于 Windows 的应用程序或完整的 Windows 桌面。用户可以连接到终端服务器来运行程序、保存文件，以及使用该服务器上的网络资源。

2）TS Web 访问

Terminal Services Web Access（TS Web Access）使用户能够通过网站（从 Internet 或 Intranet）访问 RemoteApp（TM）程序和到终端服务器的远程桌面连接。TS Web Access 还包括远程桌面 Web 连接，它使用户能够远程连接到具有“远程桌面”访问权限的任何计算机。

3）TS 授权

终端服务授权（TS 授权）管理每个设备或用户连接到终端服务器所需的终端服务客户端访问许可证（TS CAL）。使用 TS 授权在终端服务许可证服务器上安装、颁发 TS CAL，并监视其可用性。

4）TS 网关

终端服务网关（TS 网关）使经过授权的远程用户能够从可以运行远程桌面连接（RDC）客户端的任何与 Internet 连接的设备连接到内部企业网络上的资源，而不必配置虚拟专用网络（VPN）连接。

5）TS 会话 Broker

Terminal Services Session Broker（TS Session Broker）支持在服务器场中的终端服务器之间进行会话负载平衡，并支持重新连接到负载平衡终端服务器场中的现有会话。

6）TS RemoteApp

RemoteApp 程序是通过终端服务远程访问的程序，它们的行为就好像运行在最终用户的本地计算机上一样。用户可以将 RemoteApp 程序与本地程序并排运行。如果用户从同一台终端服务器运行多个 RemoteApp 程序，RemoteApp 程序将共享同一个终端服务会话。通过此功能可以节省用户会话，并且可以更快地连接到同一台服务器上的每个其他 RemoteApp 程序。

8.3　案例 1 实施过程

案例实施的总体过程如下。

（1）使用服务器管理器安装终端服务器角色服务。

（2）在终端服务器上部署安装应用程序。

（3）创建应用程序连接。

（4）远程连接访问测试。

8.3.1　任务 1：终端服务的安装

“终端服务器”角色服务在 Windows Server 2003 中称为终端服务器组件，需要通过组件添加的方式安装终端服务，而 Windows Server 2008 中增加了一个名为“服务管理器”的管理工具，可以在该控制台中集中地管理服务器角色，可以进行服务器角色的添加、删除，或者角色特性的调整等操作，相对于 Win 2000、Win 2003 中需要通过组件添加的方式安装终端服务更为友好、便利。

执行本任务时应注意下列要点。

- 计划配置的终端服务器必须是本地 Administrators 组中的成员身份，如 Administrator 或等效身份。
- 该账户必须具有强密码。
- 服务器已配置如静态 IP 地址等网络设置（本书终端服务器的 IP 是 10.0.0.3）。

若要安装终端服务器角色服务，首先将一台安装好 Windows Server 2008 的服务器加入域（不建议在域控制器上安装“终端服务器”角色服务），安装上 Web 服务器（IIS7.0）角色，然后执行下列操作。

（1）打开服务器管理器。要打开“服务器管理器”，单击“开始”，指向“管理工具”，然后单击“服务器管理器”。

（2）在左侧窗格中，右击“角色”，然后单击“添加角色”，如图 8-2 所示。

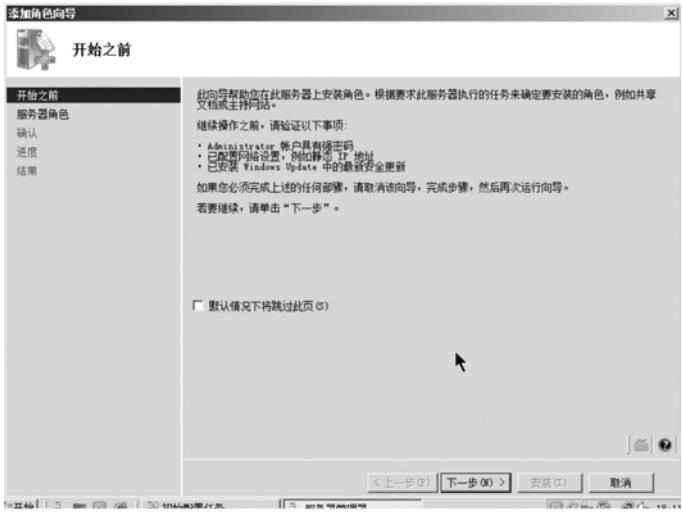

图 8-2　“添加角色向导”对话框

（3）在“添加角色向导”对话框中的“开始之前”页上，单击“下一步”按钮。

（4）在“选择服务器角色”页上的“角色”下，选中“终端服务”复选框，单击“下一步”按钮，如图 8-3 所示。

（5）在“终端服务”页上，单击“下一步”按钮，如图 8-4 所示。

（6）在“卸载并重新安装兼容的应用程序”页上，单击“下一步”按钮。

（7）在“选择角色服务”页上，必须选中“终端服务器”复选框，如果需要通过 Web 方式安全访问终端服务器等，则需要选择“TS Web 访问”和“TS 网关”复选框，然后单击“下

一步”按钮，如图 8-5 所示。

图 8-3　“选择服务器角色”页

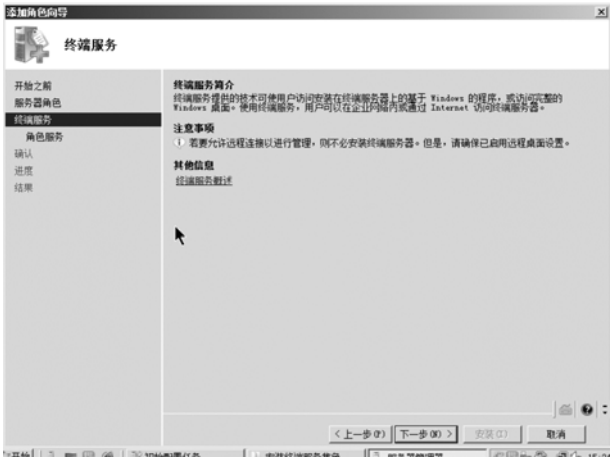

图 8-4　“终端服务”页

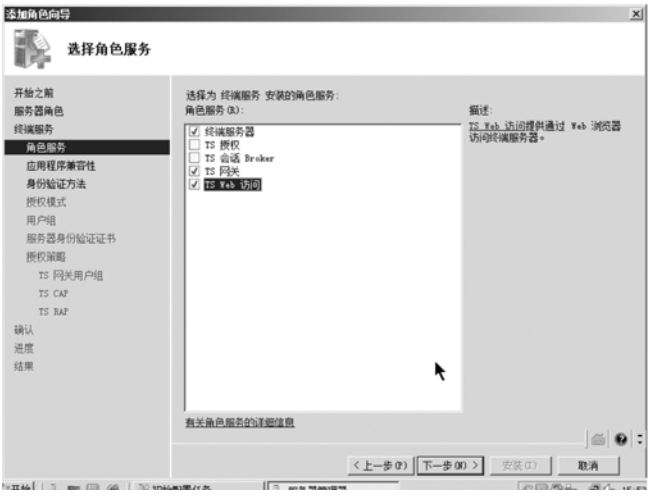

图 8-5　“选择角色服务”对话框

（8）在“卸载并重新安装兼容的应用程序”页上，系统会出现如图 8-6 所示的提示，单击“下一步”按钮。

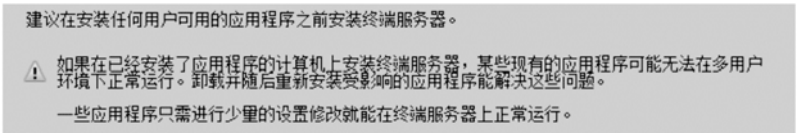

图 8-6　信息提示

（9）在“指定终端服务器的身份验证方法”页上，为终端服务器选择是否启用网络级别身份验证（NLA），如图 8-7 所示。网络级别身份验证可以在连接到终端服务器进行身份验证之前提供网络级别的验证，提高了连接的安全性。要启用 NLA 功能，还需要在服务器端的系统属性中，选择只允许 NLA 认证的用户访问终端服务器。这里选择“不需要网络及身份验证”，然后单击“下一步”按钮。

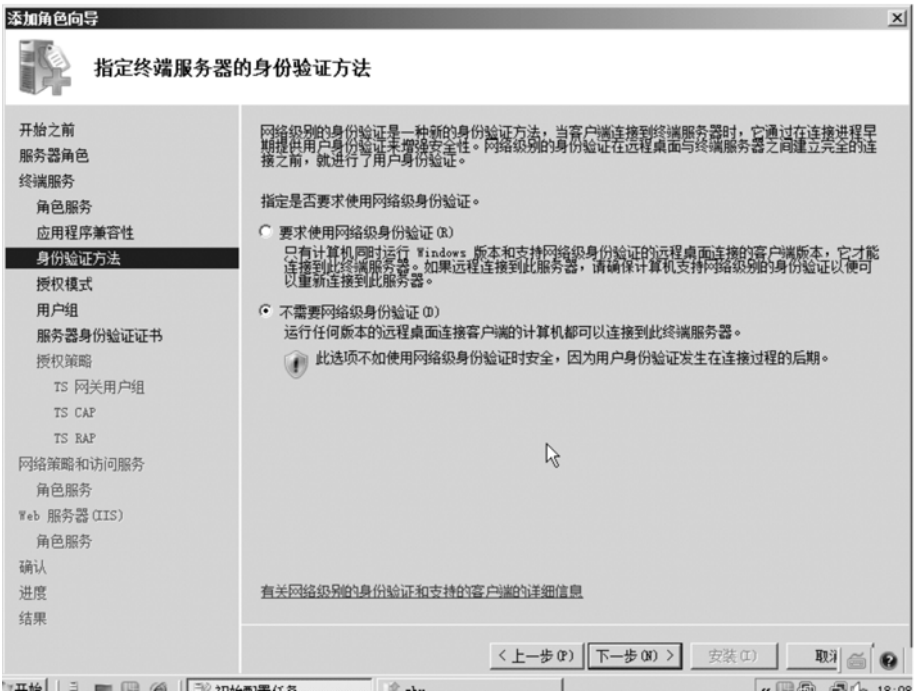

图 8-7　“指定终端服务器的身份验证方法”页

（10）在“指定授权模式”页上，选择适合的终端服务环境的授权模式，可以选择“每设备”、“每用户”或者“以后配置”，这里选择“以后配置”，如图 8-8 所示。然后单击“下一步”按钮。

（11）在“选择 SSL 加密的服务器身份验证证书”页上，选择“为 SSL 加密创建自签名证书”，如图 8-9 所示。然后单击“下一步”按钮。

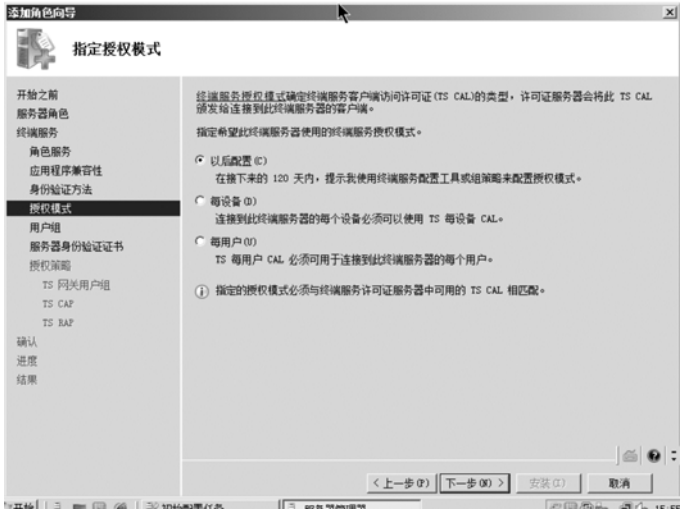

图 8-8　“指定授权模式”页

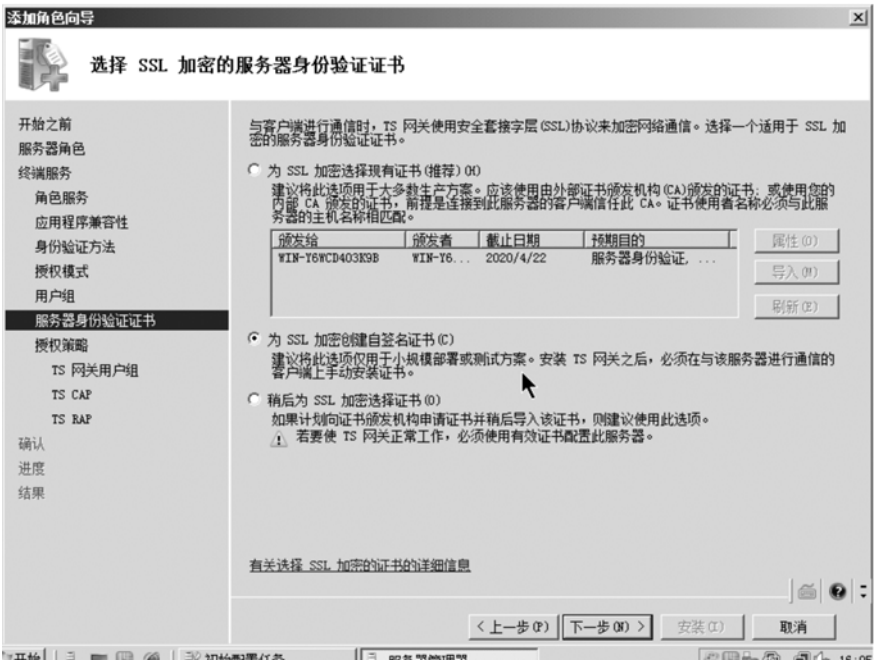

图 8-9　“选择 SSL 加密的服务器身份验证证书”页

（12）在“为 TS 网关创建授权策略”页上，选择“现在”，如图 8-10 所示。然后单击“下一步”按钮。

（13）在“选择允许访问此终端服务器的用户组”页上，选择希望能够远程连接到此终端服务器的用户或用户组，将其添加到 Remote Desktop Users 组中，如图 8-11 所示。然后单击“下一步”按钮。

（14）在“为 TS 网关创建 TS CAP”页上，选择“密码”验证模式，如图 8-12 所示。然后单击“下一步”按钮。

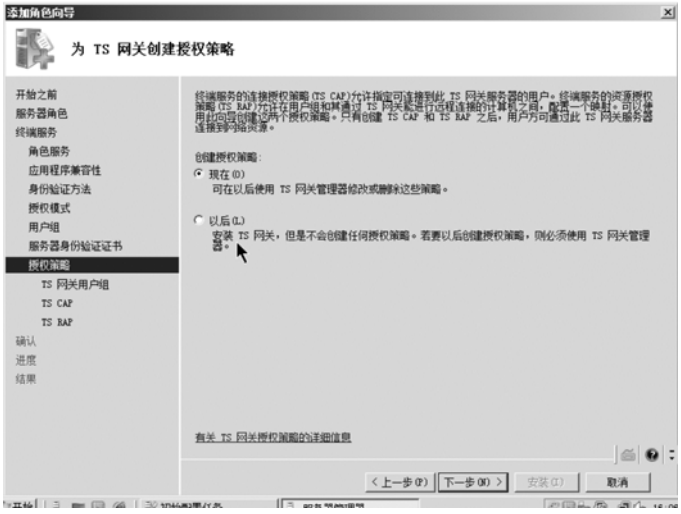

图 8-10　“为 TS 网关创建授权策略”页

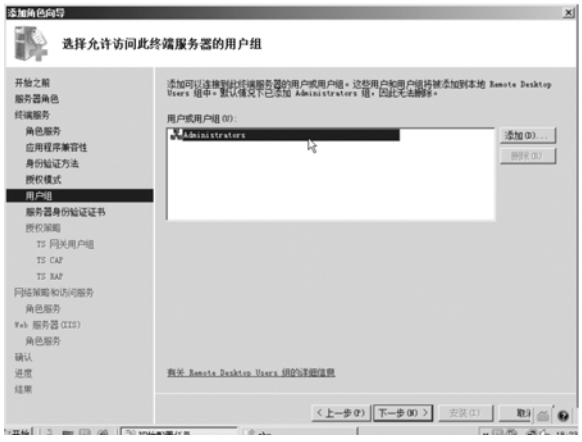

图 8-11　“选择允许访问此终端服务器的用户组”页

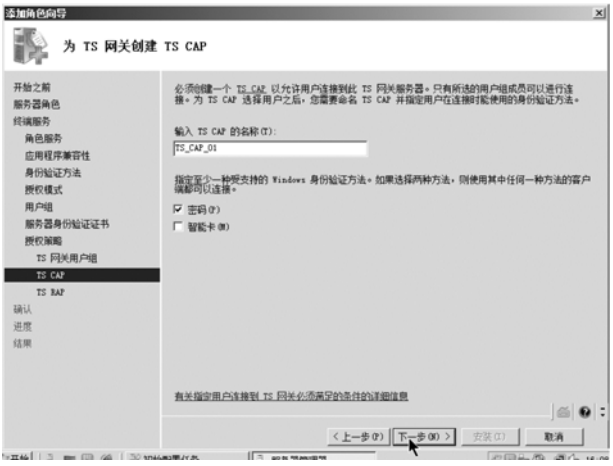

图 8-12　“为 TS 网关创建 TS CAP”页

（15）在“为 TS 网关创建 TS RAP”页上，选择“允许用户连接到网络上的任何计算机”，如图 8-13 所示。然后单击“下一步”按钮。

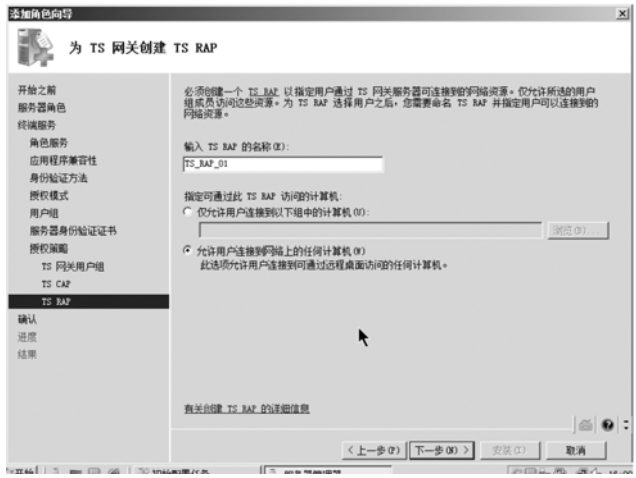

图 8-13　“为 TS 网关创建 TS RAP ”页

（16）在“确认安装选择”页上，验证是否将安装“终端服务器”角色服务，如图 8-14 所示。然后单击“安装”按钮。

图 8-14　“确认安装选择”页面

（17）在“安装进度”页上，将注明安装进度，安装过程大约需要 3 分钟。

（18）在“安装结果”页上，系统将提示用户重新启动服务器以完成安装过程。单击“关闭”按钮，然后单击“是”按钮重新启动服务器。

（19）如果系统提示其他程序仍在运行，请执行下列任意操作。

- 若要以后手动关闭程序并重新启动服务器，请单击“取消”按钮。
- 若要自动关闭程序并重新启动服务器，请单击“立即重新启动”按钮。

（20）服务器重新启动并且登录到计算机上之后，将完成安装的剩余步骤。“安装结果”页出现后，确认已成功安装了终端服务器，如图 8-15 所示。

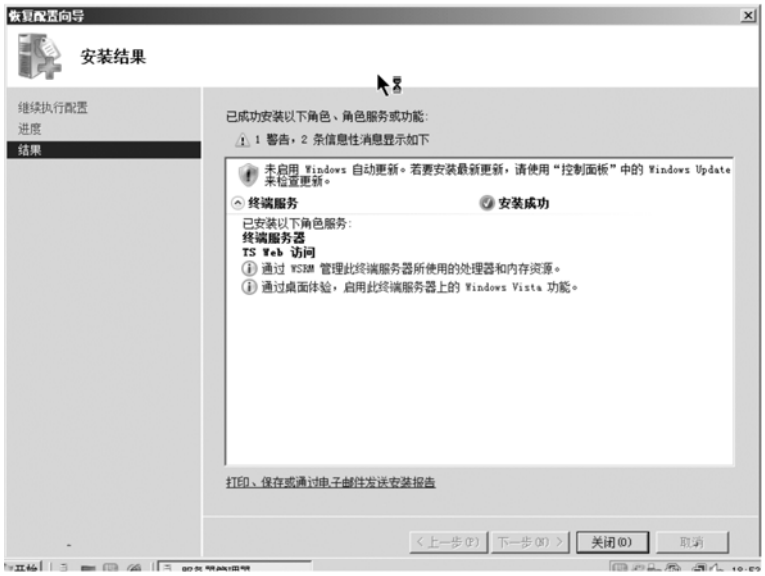

图 8-15　“安装结果”页面

还可以通过执行下列步骤确认已安装了终端服务器。

启动服务器管理器。展开“角色”，单击“终端服务”，显示“TS RemoteApp 管理器”、“TS 网关管理器”、“终端服务配置”和“终端服务管理器”都已安装，如图 8-16 所示。

图 8-16　服务器管理器

- 在“系统服务”下，确认“终端服务”的状态为“正在运行”。
- 在“角色服务”下，确认“终端服务器”的状态为“已安装”。

8.3.2　任务 2：在终端服务上部署应用程序

终端服务 RemoteApp 程序是一个通过终端服务远程访问连接的程序，用户使用 RemoteApp 进程连接时就好像运行在最终用户自己的本地计算机上一样。用户可以同时运行

RemoteApp 应用与本地应用程序。如果用户从同一台终端服务器运行多个 RemoteApp 程序，RemoteApp 程序将共享同一个终端服务会话。通过此功能可以节省用户会话，并且可以更快地连接到同一台服务器上的每个其他 RemoteApp 程序。

安装好终端服务之后，需要进行设置，使用户可以访问服务器上的 RemoteApp 应用程序，具体的设置方法如下。

（1）单击“开始”，指向“管理工具”，然后单击“终端服务”，选择“TS RemoteApp 管理器”，如图 8-17 所示。

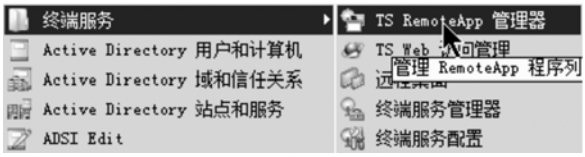

图 8-17　选择“TS RemoteApp 管理器”菜单命令

（2）在“TS RemoteApp 管理器”右侧的窗格任务栏中，选择“添加 RemoteApp 程序”，如图 8-18 所示。

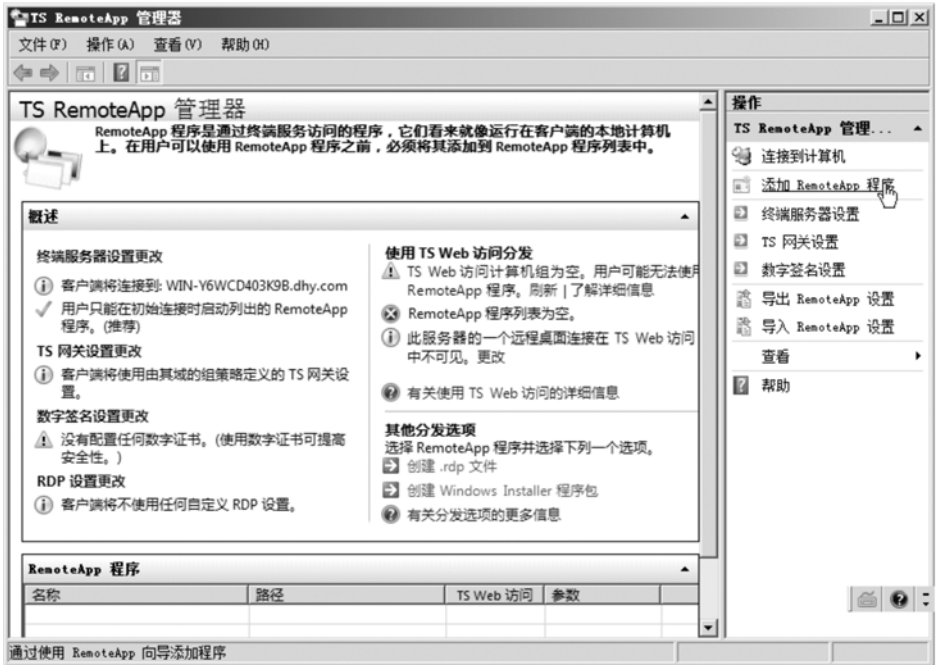

图 8-18　选择“添加 RemoteApp 程序”页面

（3）出现添加应用程序的 RemoteApp 向导，如图 8-19 所示。单击“下一步”按钮。

（4）在出现的应用程序列表中选择向用户发布的应用程序，如图 8-20 所示。单击“下一步”按钮。

（5）系统出现刚刚选择的应用程序的复查设置页，单击“完成”按钮。

（6）接下来在“TS Remote 管理器”中显示应用程序列表，如图 8-21 所示。

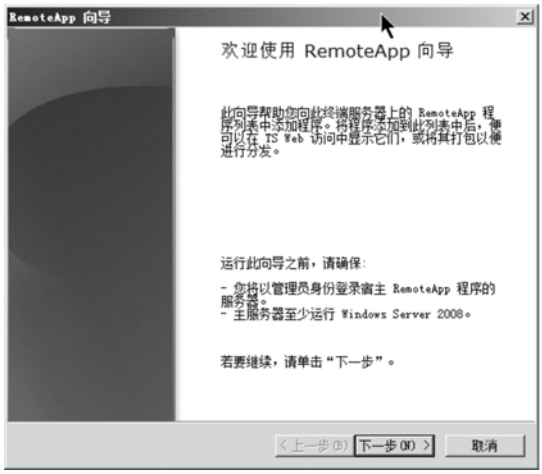

图 8-19　RemoteApp 向导

图 8-20　选择向用户发布的应用程序

图 8-21　显示应用程序列表

（7）右击选中的应用程序可以对其进行删除、创建.rdp 文件及 Windows Installer 程序包等操作，如图 8-22 所示。

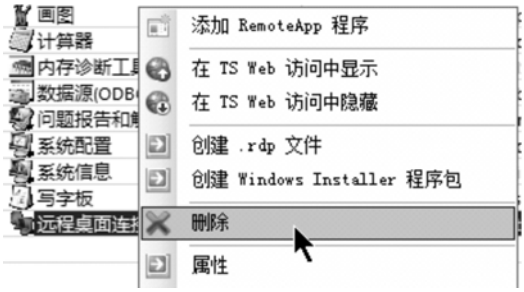

图 8-22　右键菜单

8.3.3　任务 3：创建应用程序连接

可以在应用程序列表中右击应用程序，选择将应用程序创建为 RDP 文件或 MSI 文件，然后通过 E-mail 或 U 盘分配给用户，或者通过组策略向用户进行分发。用户接收之后，可以双击 RDP 或者 MSI 文件直接打开，连接终端服务器，运行该应用程序，就像使用本地的应用程序一样，非常方便。

1．创建 MSI 格式的安装应用程序连接

在本任务中，创建一个 MSI 格式文件，可以通过 E-mail 或 U 盘分配给用户手动安装，或者通过组策略向用户进行分发，凡是在 TS Remote 管理器中的应用程序列表中显示的应用程序都可以创建为 MSI 格式文件。

（1）在“TS RemoteApp 管理器”对话框中右击选中的应用程序，如“计算器”或“写字板”。选择“创建 Windows Installer 程序包”菜单命令，如图 8-23 所示。

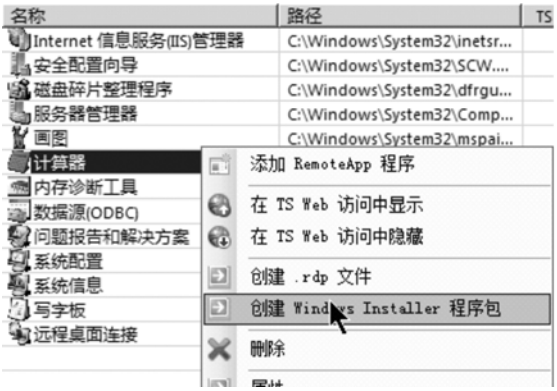

图 8-23　“创建 Windows Installer 程序包”菜单命令

（2）系统弹出添加应用程序的“RemoteApp 向导”对话框，如图 8-24 所示。单击“下一步”按钮。

（3）在出现的对话框中，输入要保存程序包的位置，如图 8-25 所示。单击“下一步”按钮。

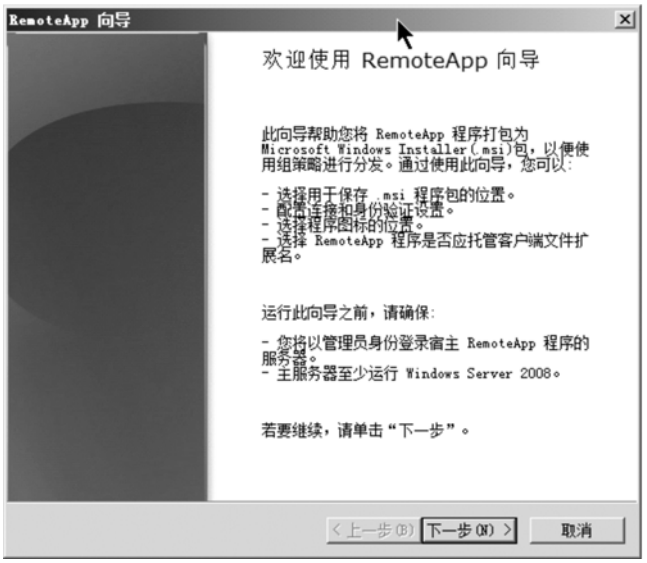

图 8-24　“RemoteApp 向导”对话框

图 8-25　保存位置对话框

（4）在接下来出现的对话框中，选择在客户端计算机上查看和安装程序包的方式，如“桌面”或“‘开始’菜单文件夹”的复选框，并输入欲显示的名称，如“远程办公室”等，如图 8-26 所示。单击“下一步”按钮。

（5）系统弹出“复查设置”页，单击“完成”按钮，如图 8-27 所示。

（6）系统弹出程序包的保存位置、名称和大小等信息，如图 8-28 所示。

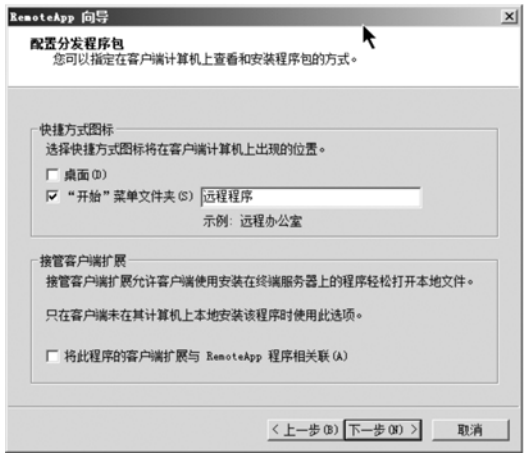

图 8-26　分发程序包对话框

图 8-27　"复查设置"页

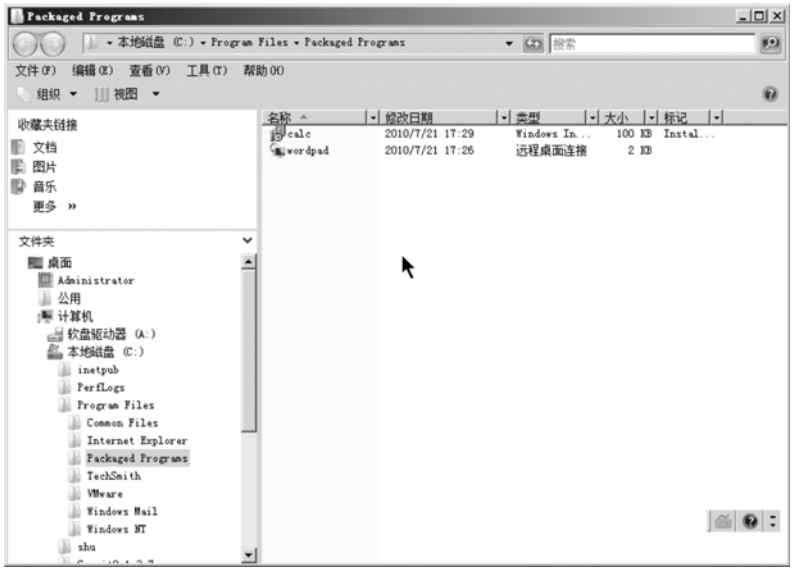

图 8-28　程序包信息页面

2．创建 RDP 文件格式的安装应用程序连接

将应用程序创建为 RDP 文件的方式可参照前面的设置，只是生成的文件格式不同，如图 8-29 所示。

图 8-29　创建为 RDP 文件的复查设置页面

8.3.4　任务 4：客户端使用 RemoteApp 程序访问测试

前面所创建的 RDP 文件和 MSI 文件，都可以通过 E-mail 或 U 盘分配给用户手动安装，或者通过组策略向用户进行分发。用户接收之后，在客户端计算机中可以双击.rdp 或者.msi 文件直接将其打开，就可以连接终端服务器，运行该应用程序了。

1．应用程序文件写字板.rdp 的远程桌面连接

（1）选择写字板.rdp 文件的“远程桌面连接”，如图 8-30 所示。

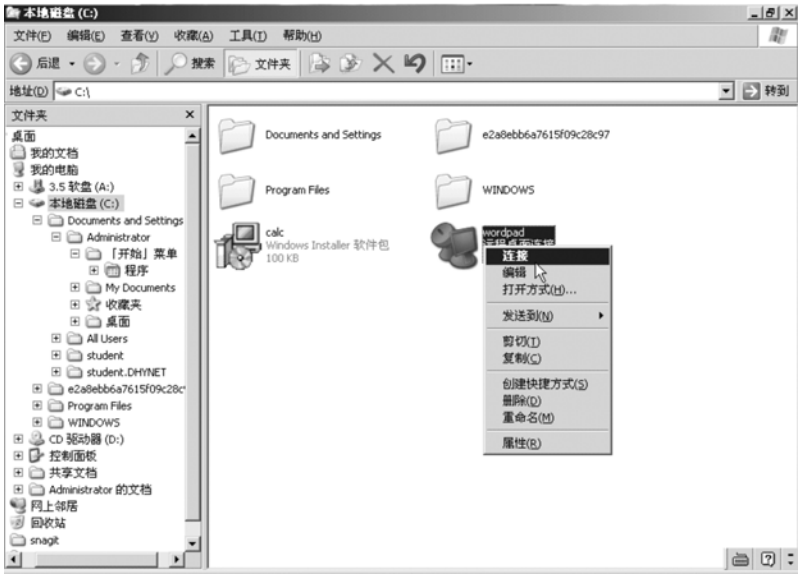

图 8-30　连接终端服务器

（2）系统会显示“远程桌面连接”对话框，如图 8-31 所示。

图 8-31　“远程桌面连接”对话框

（3）选择浏览计算机，如图 8-32 所示。

图 8-32　选择浏览计算机

（4）系统会出现“远程桌面连接安全警告”对话框，如图 8-33 所示。

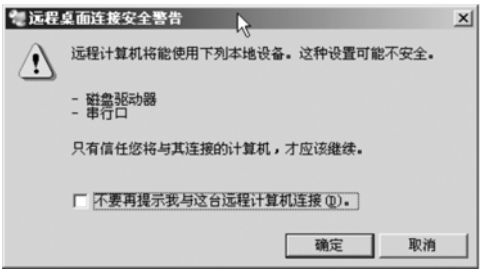

图 8-33　“远程桌面连接安全警告”对话框

（5）在接下来出现的如图 8-34 所示的对话框中，输入有效的用户名及密码之后就可以进行使用了。

图 8-34　输入信息对话框

（6）如图 8-35 所示是远程桌面连接的写字板应用界面，就像使用本地的应用程序一样，非常方便。

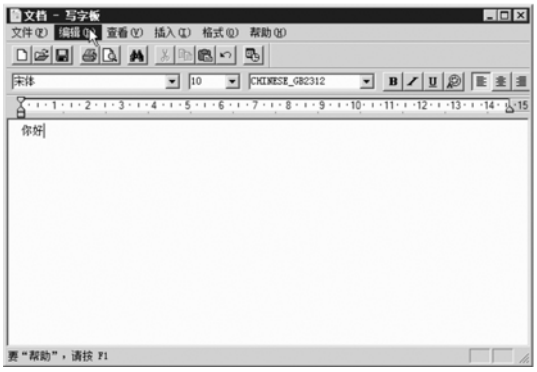

图 8-35　远程桌面连接的写字板应用界面

2．Windows Installer 程序包计算器 MSI 文件的安装

（1）右击 Windows Installer 程序包计算器 MSI 文件，选择“安装”命令，如图 8-36 所示。

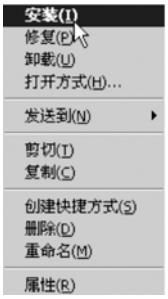

图 8-36　安装 Windows Installer 程序包计算器 MSI 文件

（2）安装结束后，在“开始”→“所有程序”菜单的下面，会出现“远程程序”→“计算器”的菜单。单击运行，如图 8-37 所示。

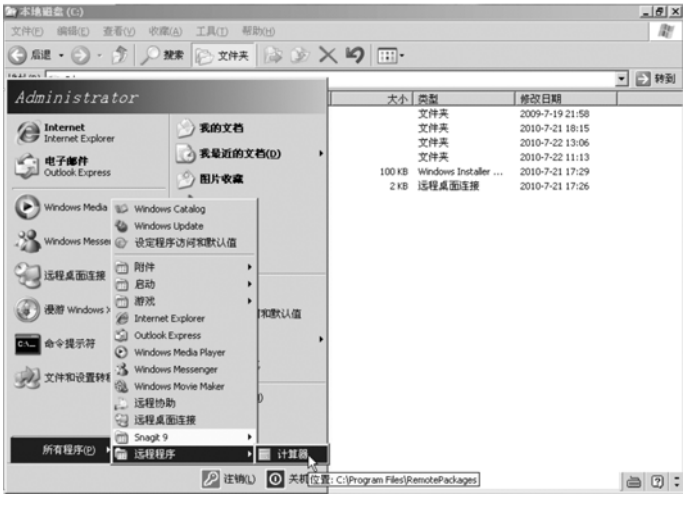

图 8-37　从开始菜单打开计算器远程程序

（3）系统会显示“远程桌面连接”对话框，如图 8-38 所示。

图 8-38　“远程桌面连接”对话框

（4）选择浏览计算机，如图 8-39 所示。

图 8-39　选择浏览计算机

（5）系统会出现“远程桌面连接安全警告”对话框，如图 8-40 所示。

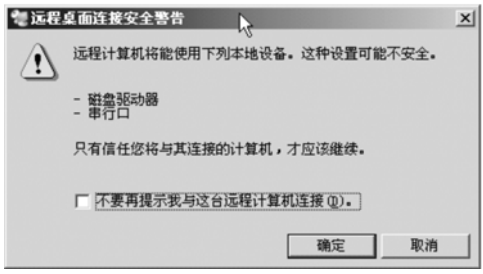

图 8-40　“远程桌面连接安全警告”对话框

（6）在接下来出现的如图 8-41 所示的对话框中，输入有效的用户名及密码之后就可以进行使用了。

图 8-41　输入信息对话框

（7）系统会弹出应用程序“计算器”的启动界面，如图 8-42 所示。

图 8-42　应用程序“计算器”的启动界面

（8）如图 8-43 所示是远程程序“计算器”的应用界面，就像使用本地的应用程序一样，非常方便。

图 8-43　远程程序“计算器”的应用界面

8.4　知识能力拓展案例 2：终端服务之实现 Web 应用程序访问和系统资源管理

8.4.1　工作情景描述

你是 DHYNET 公司的网络管理员，DHYNET 公司的业务范围遍布全国各地，员工需要经常外出，但是可以通过无线网络远程连接公司网络的服务器或办公室的计算机。员工希望能够使用内置在终端服务中的 TS Web Access 功能来实现通过 Web 方式访问单位局域网终端服务器的目的，这样的问题你该如何解决呢？

当远程访问终端服务的用户增多时，终端服务的性能就会急剧下降，你需要采取一些措施，将内存、CPU 等关键资源在应用程序、服务、进程之间进行合理分配，作为 DHYNET 公司的网络管理员，你是如何监视和分配这些资源的呢？

8.4.2　案例分析

Windows Server 2008 系统在终端服务功能方面明显得到了增强。在 Windows Server 2008 系统环境下，客户端用户能够使用内置在终端服务中的终端服务网络访问（TS Web Access）功能，实现通过 Web 方式访问单位局域网终端服务器的目的，突破了以往只能通过远程桌面连接访问终端服务器的限制，通过这种访问方式客户端用户能够享受到良好的用户体验。TS RemoteApp 管理器提供了用于将应用程序发布到 TS Web 访问的非常快速且有效的过程。可以使用 TS RemoteApp 管理器来添加为 TS Web 访问启用的 RemoteApp 程序。接下来，将 TS Web 访问安装到您希望用户通过 Web 连接的服务器上。将 TS Web 访问服务器的计算机账户添加到终端服务器上的 TS Web 访问计算机组中。最后，配置 TS Web 访问服务器，以便从单一终端服务器填充其 RemoteApp 程序列表。此外，Windows Server 2008 系统的终端服务还新增加了 TS Gateway 网关功能，该功能能够判断出客户端用户是否满足网络连接条件，并且能够确定用户究竟能够访问哪些终端服务器，从而有效保证了终端访问的安全性。

终端服务网络访问（TS Web Access）是终端服务角色，无须用户安装任何软件，就可以从网络浏览器使用终端服务远程 App 程序。拥有 TS 网络访问（TS Web Access），用户可以访问网站并获得所有可用应用列表。当用户开始所列的程序之一时，终端服务 Session 会为该用户自动开始，该用户位于基于 Windows Server 2008 的终端服务器中，该终端服务器会为该应用做主机。对用户而言，网络界面提供了集中菜单，显示了目前可用的全部远程应用 RemoteApp 程序；运行中的远程应用如同选择菜单中的程序一样简单。

Web 方式访问终端服务器是 Windows Server 2008 终端服务器中的一个亮点。通过 Web 方式访问可以获得一个应用程序列表的页面，用户使用终端服务器上的应用程序就像在本地进行应用一样，相对通过远程桌面访问更加简便。当 TS Web Access 安装到 Windows Server 2008 网络服务器后，用户可以连接 TS 网络访问服务器，并执行其上的可用远程程序。

Windows Server 2008 还新增加了 Windows 系统资源管理器（WSRM）。使用 Windows 系统资源管理器，网络管理员可以控制 CPU、内存等资源，并将其合理分配给应用程序、服务和进程。管理这些资源可以提升系统性能，并减少干扰系统其他部分的机会。也可以对于不同的用户、不同的服务根据实际情况区别实现系统资源的分配和管理，即对关键用户、关键服务要放宽资源的使用限制，而对其他次要的，或者偶发性情况占用资源比较多的服务，需要加以限制，从而减少各个服务、各个用户互相争夺资源的情况。

8.5　案例 2 实施过程

8.5.1　任务 1：实现 Web 应用程序访问

在前面的终端服务的安装中，已经安装了“TS Web 访问”的服务角色。在下面的工作中，我们将配置终端服务的 Web 访问并发布应用程序。

（1）单击“开始”，然后单击“Internet Explorer”。

（2）在地址栏中输入“http://10.0.0.3/ts”（终端服务器的 URL，本书中终端服务器的 IP 地址是 10.0.0.3），然后按回车键。

（3）在连接到终端服务器的对话框中，输入用户名和密码，如图 8-44 所示。

图 8-44　连接到终端服务器的对话框

（4）系统如果出现提示，则单击“连接”按钮，如图 8-45 所示。

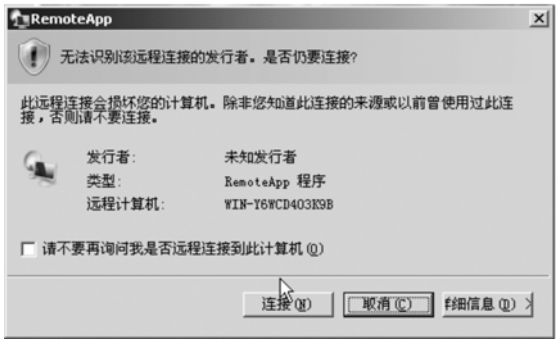

图 8-45　提示对话框

（5）系统会提示连接失败，证书存在问题，需要进行身份验证。单击“确定”按钮，如图 8-46 所示。

图 8-46　系统会提示需要进行身份验证

（6）系统会显示证书信息，单击“安装证书”按钮，如图 8-47 所示。

（7）系统会显示“证书导入向导”对话框，单击“下一步”按钮，如图 8-48 所示。

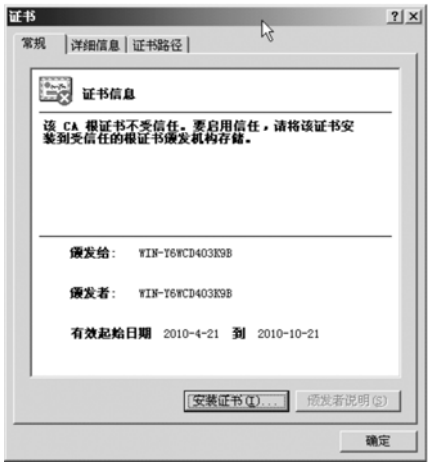

图 8-47　“安装证书”页面

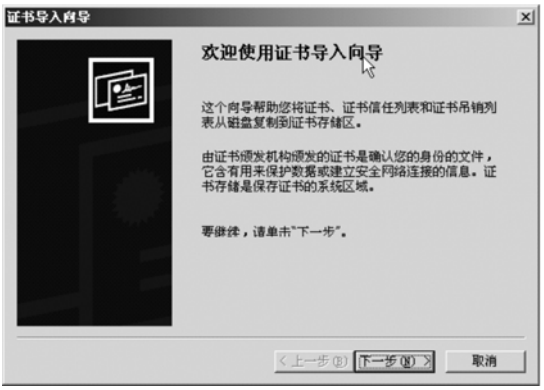

图 8-48　“证书导入向导”对话框

（8）在“证书导入向导”中，会提示证书存储区域，选择“根据证书类型，自动选择证书存储区”，单击“下一步”按钮，如图 8-49 所示。

图 8-49　选择证书存储区

（9）系统提示正在完成证书导入，单击“完成”按钮，如图 8-50 所示。

图 8-50　正在完成证书导入

（10）证书导入成功，单击“确定”按钮，如图 8-51 所示。

图 8-51　证书导入成功

（11）重新进行步骤（1）、（2）、（3），在 Internet Explorer 界面上会出现“安全警告”，如图 8-52 所示。

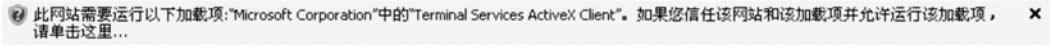

图 8-52　安全警告

（12）右击消息按钮，然后单击“运行 ActiveX 控件”。

（13）在出现的“Internet Explorer – 安全警告”对话框中，单击“运行”按钮，如图 8-53 所示。

图 8-53　“Internet Explorer 安全警告”对话框

（14）出现“TS Web 访问”网页，上面有前面终端服务已经发布的应用程序列表，如图 8-54 所示。

图 8-54　“TS Web 访问”网页

（15）单击“写字板”，会出现提示，在“RemoteApp”对话框中，单击“连接”按钮，如图 8-55 所示。

（16）在接下来的“RemoteApp”对话框中，输入用户名和密码，如图 8-56 所示。

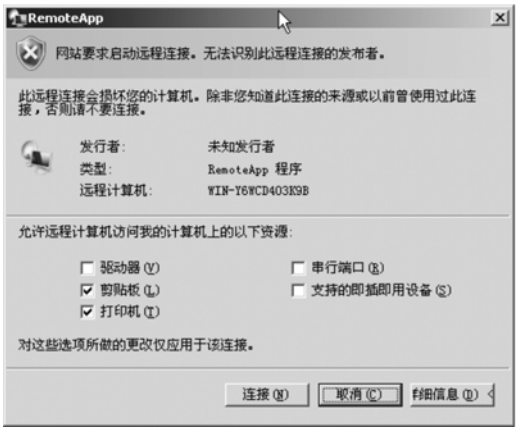

图 8-55　“RemoteApp”对话框 1

图 8-56　“RemoteApp”对话框 2

（17）系统显示终端服务 Web Access 的 RemoteApp 正在启动，如图 8-57 所示。

图 8-57　RemoteApp 启动对话框

（18）接下来就会出现 Web Access 的 RemoteApp 的写字板应用界面，就像使用本地的应用程序一样，非常方便，如图 8-58 所示。

图 8-58　Web Access 的 RemoteApp 的写字板应用界面

8.5.2　任务 2：使用 Windows 系统资源管理策略

在这项任务中，您将执行 Windows 系统资源管理策略，确保所有会话将享有平等的处理器处理时间。这将使访问终端服务器的所有用户都会感到单个用户运行的可能试图占用更多服务器资源的应用程序的影响。

（1）单击“开始”，指向“管理工具”，然后单击“服务器管理器”。

（2）在左侧窗格中，右击“功能”，然后单击“添加功能”，如图 8-59 所示。

（3）在“功能”列表中，选择“Windows 系统资源管理器”复选框，如图 8-60 所示。

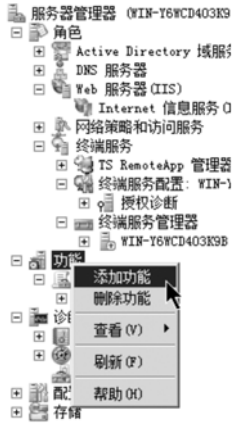

图 8-59　“添加功能”菜单

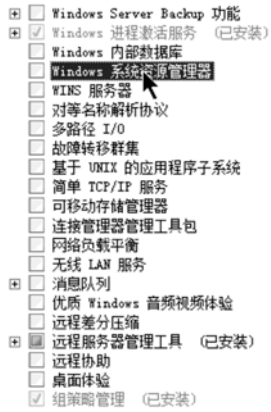

图 8-60　“功能”列表

（4）在“添加功能向导”对话框中，单击“添加必需的功能”按钮，如图 8-61 所示。

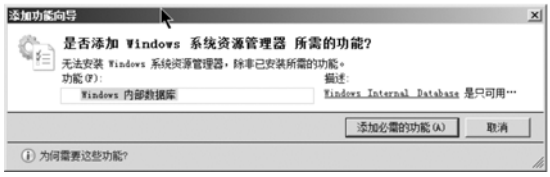

图 8-61　信息提示对话框

（5）系统会自动添加“Windows 内部数据库”复选框，如图 8-62 所示。

（6）在提示确认安装时，单击“安装”按钮（安装通常需要几分钟）。安装完成后单击“关闭”按钮。

（7）系统重新启动后，在“开始”菜单中，指向“管理工具”，然后单击“Windows 系统资源管理器”，如图 8-63 所示。

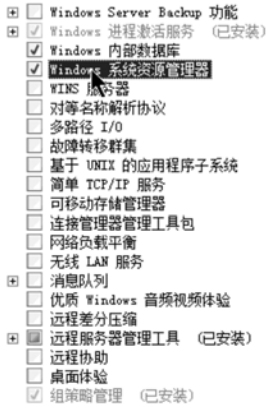

图 8-62　自动添加了必需的功能

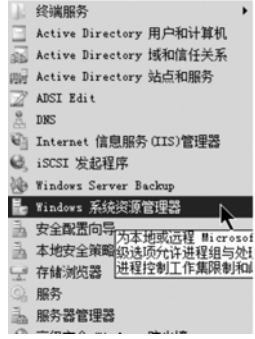

图 8-63　选择“Windows 系统资源管理器”

（8）在启动后的“Windows 系统资源管理器”中的“连接到计算机”对话框中，单击“连接”按钮，如图 8-64 所示。

图 8-64　“连接到计算机”对话框

（9）在“Windows 系统资源管理器”中，展开“资源分配策略”。

（10）在展开的树中，选择“Equal_Per_Process（管理）”，如图 8-65 所示。

（11）在“Equal_Per_Process（管理）”右侧的内容中，选择“设置为管理策略”，如图 8-66 所示。

图 8-65　资源分配策略选择

图 8-66　选择“设置为管理策略”

（12）在“警告”对话框中，单击“确定”按钮，如图 8-67 所示。

（13）在“Windows 系统资源管理器”页面的内容窗格中，单击“资源监视器”，如图 8-68 所示。

图 8-67　“警告”对话框

图 8-68　选择“资源监视器”

（14）在资源监视器上，添加一个计数器，如图 8-69 所示。

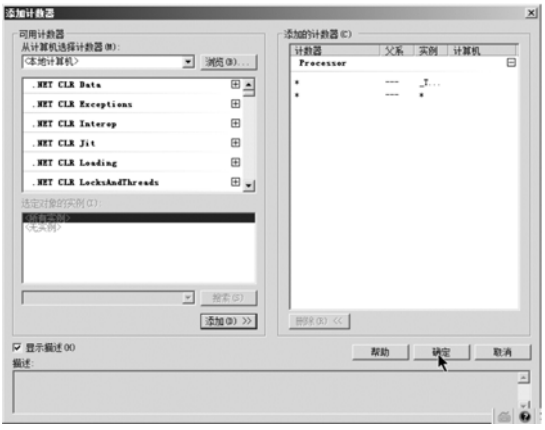

图 8-69　添加计数器

（15）在如图 8-70 所示的资源监视器上，显示了系统的 CPU% Equal_Per_Process 情况。

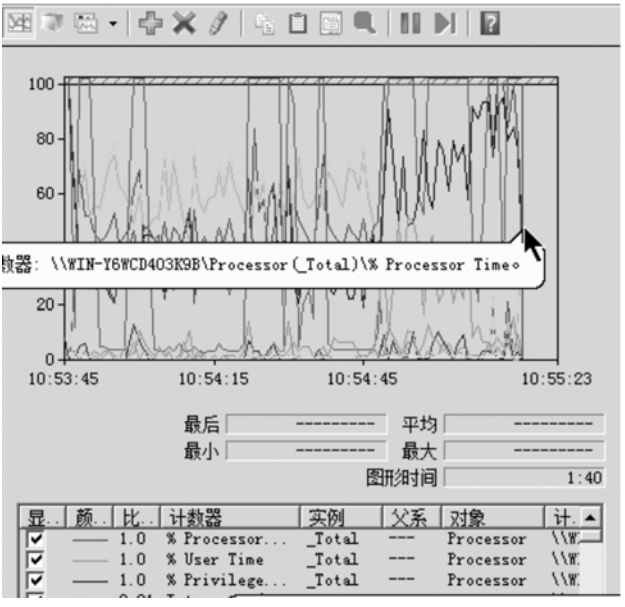

图 8-70　资源监视器监视画面

（16）在图 8-71 中显示了 WSRM 监测的所有会话都有均等占用 CPU 的机会。

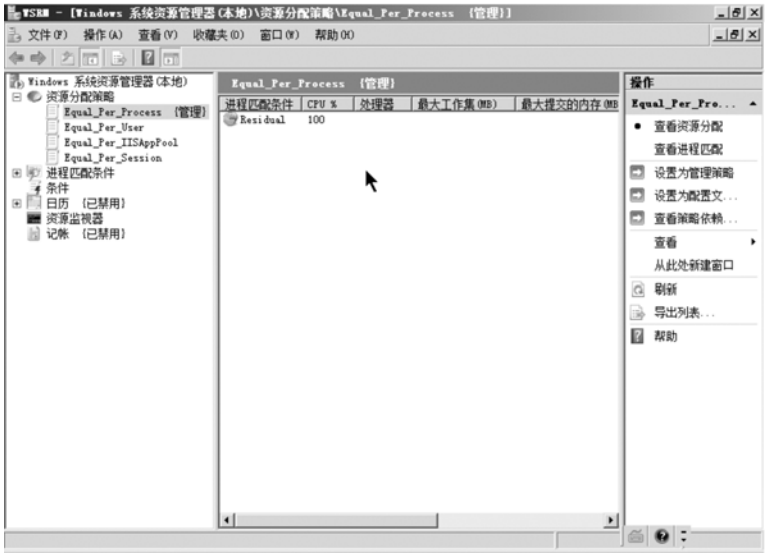

图 8-71　WSRM 监测的会话信息

8.6　项目完成结论

在 Windows Server 2008 中，一改传统的通过组件添加来安装终端服务的方式，以新增加的“服务管理器”的管理工具来安装和部署终端服务，非常方便。而且终端服务的连接也非常方便，既可以通过 Internet 利用远程桌面，也可以使用.rdp 文件或.msi 文件的方式，还可以通过 Web 等方式进行连接，运行应用程序，保存公司文件，从公司网络内部访问终端服务器。

为解决安全连接问题，还可以配置终端服务网关、证书服务器等进行多重认证，具体配置的方法用户可以根据 TS Remote Manager 中的向导进行配置。此外，Windows Server 2008 终端服务还支持单点登录功能，可以免去反复输入用户名和密码的操作，并可以在“服务管理器”中启用 Desktop Experience 特性，使用户连接到终端服务器后可以获得类似 Vista 或 Win7 的桌面效果，这些功能给用户带来了更佳的用户体验。

8.7　练 习 案 例

WTO 公司有多台服务器和计算机，它们使用了微软公司的软件产品，包括操作系统、办公软件等。你需要部署通过终端服务远程 Web Access 访问连接的程序，以使公司遍布全国各地的员工可以通过网络远程连接。

另外，为防止远程访问终端服务的用户增多时，终端服务的性能下降，需要采取一些措施，将内存、CPU 等关键资源在应用程序、服务、进程之间进行合理分配，作为 WTO 公司的网络管理员，你应该如何监视和分配这些资源呢？

根据所学的知识，实现公司的要求。

8.8　课 后 习 题

1．公司为什么要使用终端服务？
2．什么是终端服务器？
3．终端服务所使用的默认端口是多少？
4．终端服务主要应用在哪里？
5．终端服务都有哪些角色服务？
6．终端服务 TS Web 访问是如何实现的？
7．终端服务使用 TS 网关有什么益处？
8．为什么说终端服务有助于提高用户的工作效率？

项目 9　WSUS 服务的安装、配置与管理

WSUS（Windows Server Update Services）支持微软公司全部产品的更新，包括 Office、SQL Server、MSDE 和 Exchange Server 等内容。通过 WSUS 这个内部网络中的 Windows 升级服务，所有 Windows 更新都可集中下载到内部网的 WSUS 服务器中，网络中的客户机可通过 WSUS 服务器来得到更新。这在很大程度上节省了网络资源，避免了外部网络流量的浪费，并且提高了内部网络中计算机更新的效率。

知识点、技能点

- WSUS 服务器的安装
- WSUS 服务器的管理
- WSUS 客户端的设置

9.1　引例：为什么要使用 WSUS（WHY）

任何软件都不是完美无缺的，微软公司的产品也不例外。当微软公司发现它们的产品有缺陷或者漏洞时，就会发布补丁更新。用户通常各自直接到微软公司的网站上去自动更新，或手动更新，也有到其他网站上下载补丁更新的。

在公司里，员工各自下载补丁更新显然有两个缺点，一是浪费流量。同一个补丁，1 000 台计算机各下载一次，就要下载 1 000 次。二是效率不高，特别是在网速不快的情况下。

解决这个问题方法是，在公司搭建 WSUS 服务器，所有 Windows 更新都集中下载到内部网的 WSUS 服务器中，而内部网络中的客户机都通过 WSUS 服务器来得到更新。这在很大程度上节省了网络资源，避免了外部网络流量的浪费，并且提高了内部网络中计算机更新的效率。

9.2　案例 1：WSUS 服务的基本管理

9.2.1　工作情景描述

DHYNET 公司有一千多台计算机，软件使用了微软公司的产品，包括操作系统、办公软件等。为保证软件的及时升级，所有计算机都设置了自动更新功能。某个星期一的上午，网管员发现网络流量很高，经过检查分析，是微软公司在星期日发布了一个重要安全补丁，星期一员工开启计算机后，所有计算机都在下载补丁自动升级。过高的网络流量造成了网络负载过重，影响了公司的正常工作。该如何解决这样的问题呢？

9.2.2　案例分析

软件产品通常要及时更新才能防止木马病毒等的入侵，才能使用新的技术和功能。DHYNET 公司使用微软公司的产品比较多，微软公司一发布软件更新，公司的计算机就会在同一时间或者临近的时间到微软公司的更新网站上下载新的更新。考虑到 DHYNET 公司规模较大，为了节省网络流量，同时也提高更新补丁下载的效率，应该为公司搭建 WSUS 服务器。

9.2.3　相关知识

WSUS 3.0 SP2 是微软发布的最新版本的 WSUS。

1．WSUS 服务器软件先决条件

需要使用以下受支持的操作系统之一：

- Windows Server 2008 R2；
- Windows Server 2008 SP1 或更高版本；
- Windows Server 2003 SP1 或更高版本；
- Windows Small Business Server 2008；
- Windows Small Business Server 2003；
- IIS 6.0 或更高版本；
- Microsoft .NET Framework 2.0 或更高版本。

需要使用以下受支持的数据库之一：

- Microsoft SQL Server 2008 精简版、标准版或企业版；
- SQL Server 2005 SP2；
- Windows 内部数据库。

如果尚未安装受支持的 SQL Server 版本，则 WSUS 3.0 SP2 安装向导将安装 Windows 内部数据库。

Windows Server 2008 R2 需要 WSUS 3.0 SP2。如果您安装的是 Windows Server 2008 R2，则应该安装 WSUS 3.0 SP2。请不要在 Windows Server 2008 R2 上安装 WSUS 3.0 SP1。

2．WSUS Server 硬件要求

系统分区和安装 WSUS 3.0 SP2 的分区都必须采用 NTFS 文件系统进行格式化。

系统分区上至少有 1 GB 的可用空间。

存储数据库文件的卷上至少有 2 GB 的可用空间。

存储内容的卷上至少有 20 GB 的可用空间，建议可用空间为 30 GB。

WSUS 3.0 SP2 不能安装在压缩的驱动器上。

9.3　案例 1 实施过程

9.3.1　任务 1：安装和初次配置 WSUS 服务器

在开始安装之前，安装 WSUS 的计算机必须连接到 Internet 上。

（1）单击“开始”→“服务器管理器”，在“服务器管理器”主窗口的“角色摘要”下，单击“添加角色”。在“添加角色向导”中，单击“下一步”按钮。在服务器“角色”列表中，选择“Windows Server Update Services”，单击“添加必需的角色服务”，如图 9-1 所示。

（2）单击 4 次“下一步”按钮，再单击“安装”按钮。

说明：上述安装过程是边下载边安装 WSUS 3.0 SP2，WSUS 3.0 SP2 是从微软的网站上下载的。如果下载比较慢，费时较长，可以先安装必要的 IIS 服务后，从其他地方下载 WSUS 3.0 SP2，然后从本地安装。

图 9-1　添加 WSUS 角色

（3）在弹出的“Windows Server Update Services 3.0 SP2 安装向导”中单击“下一步”按钮，如图 9-2 所示。

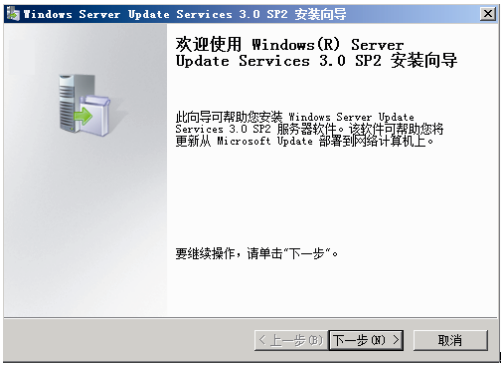

图 9-2　WSUS 3.0 SP2 安装向导

（4）在“许可协议”对话框中，选中“我接受许可协议条款”。剩下步骤采用默认安装即可，不再赘述。

（5）安装完成后，会自动启动“Windows Server Update Services 配置向导”，如图 9-3 所示。如果以后要重新运行此向导，请单击“开始”→“管理工具”→“Windows Server Update Services”，然后展开到“选项”→“WSUS 服务器配置向导”。请认真阅读对话框中的文字，确保 WSUS 服务器能够连接到 Microsoft Update，确保 WSUS 服务器的防火墙能够允许客户端访问到它。单击“下一步”按钮。

（6）在图 9-4 中选择上游服务器。WSUS 服务器是级联的，Microsoft Update 是所有 WSUS 服务器的源头，你的 WSUS 服务器可以从 Microsoft Update 获取更新，也可以从你知道的其他 WSUS 获取更新。选择后单击“下一步”按钮。

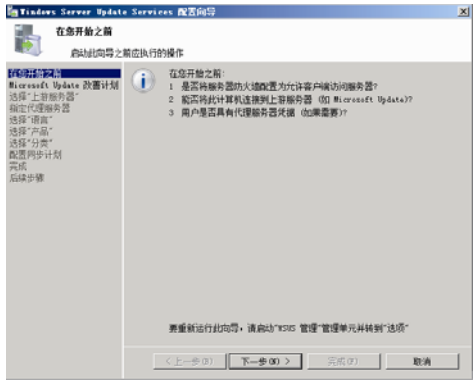

图 9-3　阅读注意事项

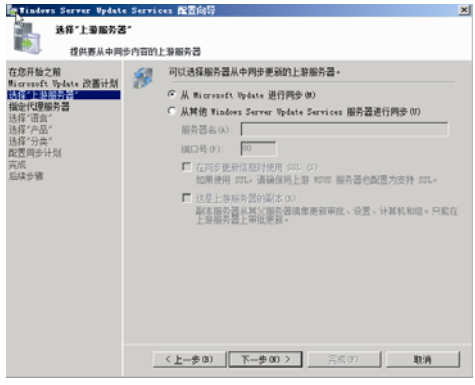

图 9-4　选择上游服务器

（7）如果你的 WSUS 服务器需要通过代理才能连接到 Microsoft Update，请在图 9-5 中进行相应设置，否则直接单击“下一步”按钮。

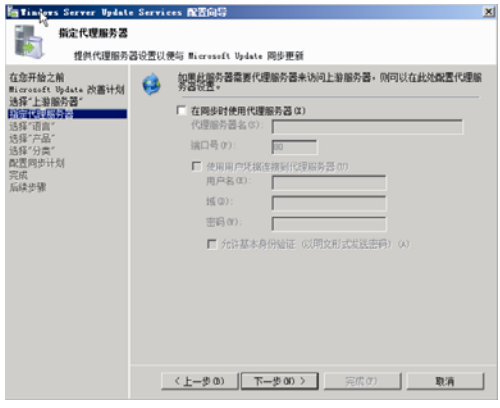

图 9-5　设置代理

（8）在图 9-6 中单击“开始连接”按钮。完成后单击“下一步”按钮。

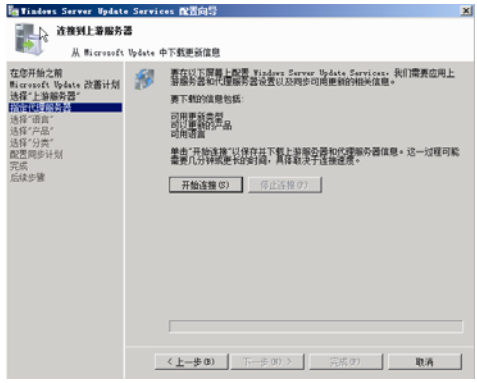

图 9-6　开始连接

（9）在图 9-7 中选择语言，选中“中文（简体）”。当然如果公司中有其他语言的微软产品，也要做相应选择。单击“下一步”按钮。

图 9-7　选择语言

（10）在图 9-8 中选择产品。这里要根据公司使用微软产品的情况来进行选择。单击“下一步”按钮。

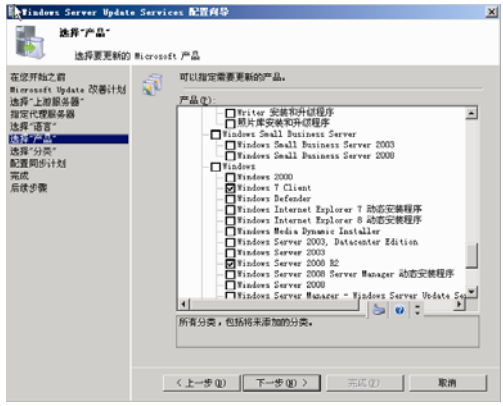

图 9-8　选择产品

（11）在图 9-9 中选择分类，即所要下载的更新的分类。根据需要选择即可。

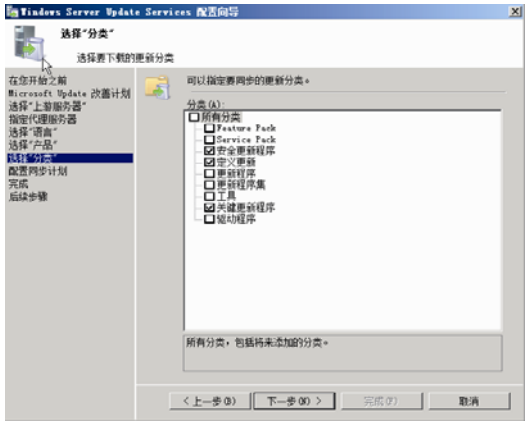

图 9-9　选择分类

（12）在图 9-10 中设置同步计划，选择“手动同步”或者“自动同步”，为了管理方便这里设置为“自动同步”。单击两次“下一步”按钮，再单击“完成”按钮。

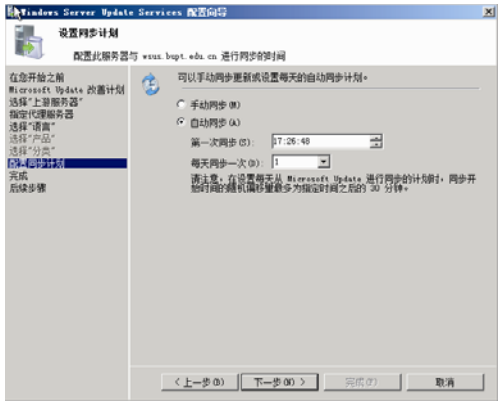

图 9-10　选择同步方式

（13）系统自动弹出的 WSUS 控制台如图 9-11 所示。第一次安装后会自动弹出 Update Services 控制台，在其他情况下要打开此控制台，请单击“开始”→“管理工具”→“Windows Server Update Services”。

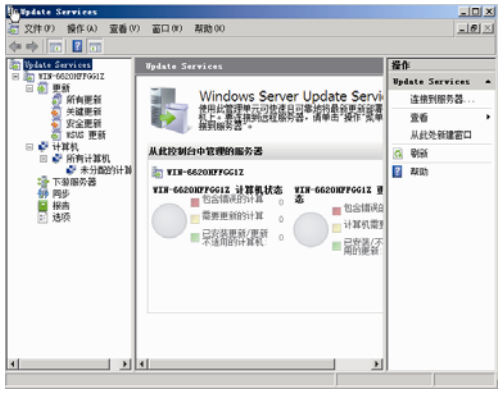

图 9-11　WSUS 控制台

9.3.2　任务 2：安装和配置客户端计算机

通常 WSUS 用于公司内部，所以这里主要叙述在域环境中如何配置 WSUS 客户端。域环境中配置 WSUS 客户端主要通过组策略来配置。

下面的配置在域控制器中完成。

（1）为 WSUS 客户端建立组织单位。单击“开始”→“管理工具”→“Active Directory 用户和计算机”，右击域名，选择“新建”→“组织单位”，输入组织单位名称，如“WSUS Windows 7”。

（2）把 WSUS 客户端加入到所建客户端中。选中组织单位“Computers”，右击要加入组织单位 WSUS Windows 7 的计算机，选择“移动”，在“移动”对话框中选择“WSUS Windows 7”。

（3）下面设置组策略。单击“开始”→“管理工具”→“组策略管理”，展开到“WSUS Windows 7”，右击“WSUS Windows 7”，选择“在这个域中创建 GPO 并在此处链接”，如图 9-12 所示。

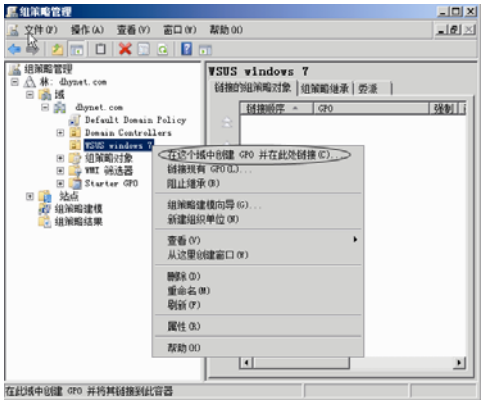

图 9-12　新建组策略

（4）在“新建 GPO”对话框中输入“名称”，如“WSUS GPO”，如图 9-13 所示，单击“确定”按钮。

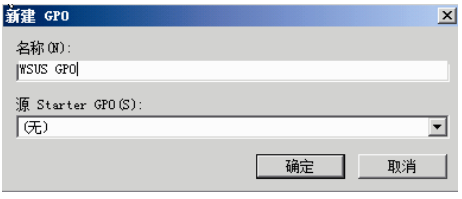

图 9-13　命名组策略

（5）右击新建的组策略对象“WSUS GPO”，选择“编辑”，在“组策略编辑器”中依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→“Windows Update”，如图 9-14 所示。

（6）在图 9-14 右侧的控制面板中双击“配置自动更新”，弹出“配置自动更新 属性”对话框，选中“已启动”，并将“配置自动更新”设置为“4-自动下载并计划按装”，这个选项使客户机能够自动下载并安装更新，当然也可以根据情况选择其他选项，单击“下一个设置”按钮，如图 9-15 所示。

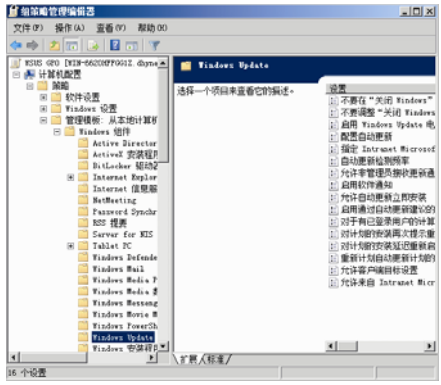

图 9-14　编辑组策略

图 9-15　设置自动更新

（7）在图 9-16 中选中“已启用”，并输入“http://win-08-wsus”，“win-08-wsus”是 WSUS 服务器的计算机名，输入“http://WSUS 服务器”的 IP 地址也行。这项设置的作用是设置客户端到 WSUS 服务器上下载 Microsoft 更新，而不是到 Microsoft Update 上下载更新。单击两次“下一个设置”按钮。

图 9-16　设置更新服务器

（8）在如图 9-17 所示的“允许非管理员接收更新通知属性”对话框中选择“已启用”。这项设置允许非管理员接收更新通知，因为在域环境中，大部分用户是非管理员，单击“确定”按钮。

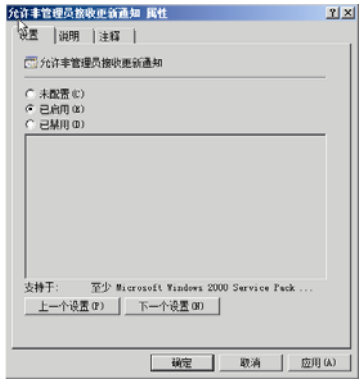

图 9-17　允许非管理员接收更新

（9）关闭“组策略编辑器”和“组策略管理”控制台。

一般情况下，组策略要等一段时间才能生效。要使组策略立即生效，可在域控制器上的命令行中使用“gpupdate /target:computer”命令刷新组策略，在 WSUS 客户的命令行中使用“gpupdate /target:computer”命令刷新组策略，并使用“wuauclt -detectnow –reauthorization”命令检测 WSUS 服务器。

如果不在域环境中，可以编辑本地策略来设置 WSUS 客户端。在 Windows 7 中打开本地策略的方法是，单击“开始”→“运行”，输入“mmc”，按回车键，在控制台中添加“组策略对象编辑器”→“本地计算机”即可。编辑的方法与在域控制器中基本一致，这里不再赘述。

通过以上配置后，再来看一下 WSUS 客户端的情况。以 Windows 7 为例。

（1）单击“开始”→“所有程序”→“Windows Update”→“检查更新”，如图 9-18 所示。

图 9-18　手动更新

（2）如图 9-19 所示是更新之后的情况。

图 9-19　更新后的情况

（3）如图 9-20 所示是 WSUS 服务器的情况，可以看出计算机 win-7 已经注册到了 WSUS 服务器中。

图 9-20　在 WSUS 上注册的客户

9.4　知识能力拓展案例 2：自动更新的测试和审批

9.4.1　工作情景描述

DHYNET 公司财务部的某个软件在某一天都不能使用了。网络管理员通过查看“事件查看器”得知，这些计算机在当天的凌晨都自动完成了微软的某个更新。公司使用 WSUS 服务器对公司的所有微软产品进行更新。管理员判断很可能是微软的这个更新和公司的该软件不兼容造成的。通过还原系统，公司的该软件又能正常使用了。能否在大面积使用更新之前，先进行测试，待测试无误后再进行大面积更新呢？

9.4.2　案例分析

可以通过下面的方法解决上面出现的问题。设置测试组，测试成功后，再对同类计算机进行全面更新。

对测试组的审批和对普通组的审批没有什么区别，只是要先对测试组更新，如果更新后没有出现问题，再对普通组进行更新即可。这对于较大的公司还是非常有必要的。

9.5　案例 2 实施过程

下面以测试组为例说明如何审批，命名测试组为“t-win 7”。下面的配置在 WSUS 服务器上进行。

（1）新建计算机组。单击“开始”→“管理工具”→“Windows Update Services”，在打开的对话框中展开“计算机”→“所有计算机”，右击“所有计算机”，选择“添加计算机组”，在弹出的“添加计算机组”对话框中输入要添加的计算机组的“名称”，如“t-win 7”，然后单击“添加”按钮，如图 9-21 所示。

（2）为计算机组 t-win 7 添加成员。选中“所有计算机”，在中间面板中右击要添加到 t-win 7 的计算机，选择“更改成员身份”，如图 9-22 所示。

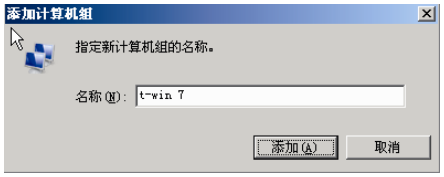

图 9-21　命名计算机组

图 9-22　更改成员身份

（3）在图 9-23 中选中“t-win 7”，单击“确定”按钮。

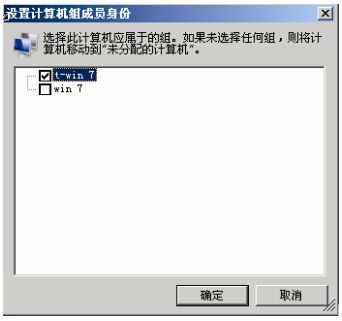

图 9-23　选择新的计算机组

（4）审批更新。在“Update Service”中展开“更新”，在中间面板中右击所要审批的更新，在弹出的“审批更新”对话框中右击“t-win 7”，选择“已审批进行安装”，如图 9-24 所示。单击“确定”和“关闭”按钮。

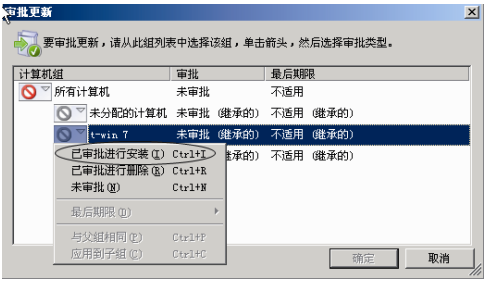

图 9-24　审批更新

下面叙述其他的一些 WSUS 常规管理。

1．同步 WSUS 服务器

在“Update Services”树中，展开要同步的服务器。右击“同步”，然后单击“立即同步”。也可以从主页中进行同步。在“结果”窗格的“同步状态”下面单击“立即同步”。

2．新建自动审批规则

（1）单击“开始”→“管理工具”→“Windows Update Services”，在打开的对话框中展开到“选项”，在中间面板中单击“自动审批”，如图 9-25 所示。

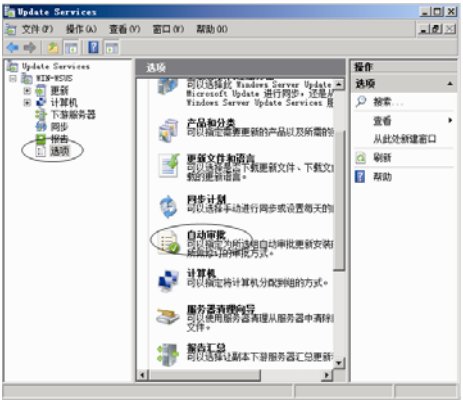

图 9-25　自动审批

（2）在“自动审批”对话框中单击“新建规则”，如图 9-26 所示。

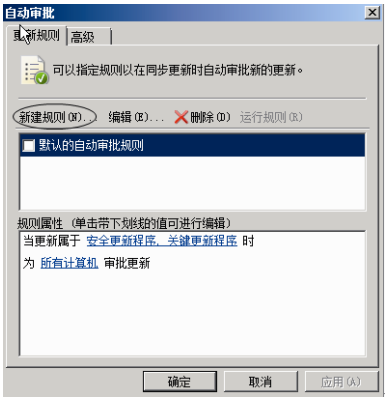

图 9-26　新建自动审批规则

（3）在“添加规则”对话框中的“步骤 3：指定名称”文本框中输入规则名称，如“windows 7”。在“步骤 1：选择属性”中可以根据情况选中其中的复选框，3 个复选框分别设置更新的分类、更新的产品和更新发生的时间。如果不选中任何一个，默认对应于任何分类、任何产品和所有计算机。选中后，可以对相应的选项进行设置，如设置产品，单击“步骤 2：编辑属性”中的“任何产品”，如图 9-27 所示。

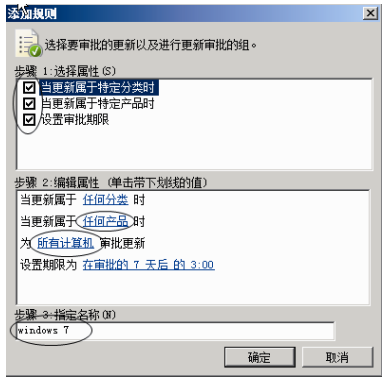

图 9-27　设置新的审批规则属性

（4）在图 9-28 中选择需要的产品，如“Windows 7 Client”，单击“确定”按钮。

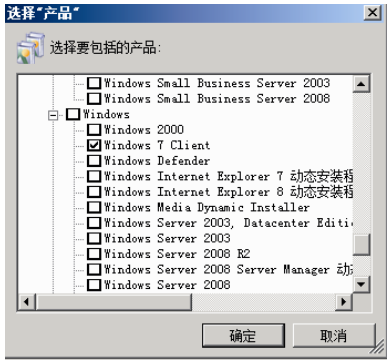

图 9-28　选择产品

（5）在图 9-29 中单击“所有计算机”，在图中选择所要的计算机组，如前面新建的“windows 7”，单击两次“确定”按钮。

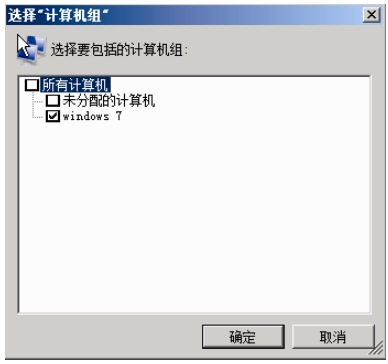

图 9-29　选择计算机组

3．运行报告

必须先安装 Report Viewer，才能查看运行报告。

借助于从 Windows Server Update Services（WSUS）3.0 中获得的报告，您可以监视通过服务器管理的计算机和 WSUS 服务器的更新、计算机，以及同步结果，也可以选择从连接到您的

服务器的下游服务器中汇总数据。WSUS Reporters 安全组的成员具有运行和查看 WSUS 报告的权限。

您可以从 WSUS 控制台中的不同位置来访问计算机和更新状态。在任何计算机或更新视图中，您都可以选择一个或多个计算机或更新，右击它们，然后单击“状态报告”。该报告将显示所选项目的状态，并允许您选择更多项或对结果进行筛选。

也可以从“Update Services”树的“报告”节点中生成报告。从此节点中获得的报告可划分为以下类别。

- 更新：更新状态摘要、更新详细状态、更新表格状态和已审批更新的更新表格状态。
- 计算机：计算机状态摘要、计算机详细状态、计算机表格状态和已审批更新的计算机表格状态。
- 同步：同步结果。

运行报告之后，您可以单击“报告视图”在现有数据的“摘要”、“详细信息”和“表格”模式之间进行切换。

有关每个报告的详细信息，请参见运行报告下面的主题。

4．更新状态术语

WSUS 可报告多种更新状态。如表 9-1 所示定义了 WSUS 可以报告的每种可能的更新状态。通常，WSUS 显示特定计算机的更新状态（如一台计算机上的更新状态）或计算机组的更新状态（如已安装更新的计算机组中的 5 台计算机的状态）。

表 9-1　WSUS 报告的可能更新状态

更 新 状 态	描　　述
已安装	计算机上安装了更新
需要	提及一台计算机的状态时，“需要”表示应该在计算机上安装更新。提及计算机组的状态时，“需要”列显示组中应该安装更新的计算机数
失败	无法在计算机上进行更新
无状态	WSUS 无法获取更新状态。通常，这表示将更新与 WSUS 服务器进行同步后，计算机尚未连接 WSUS 服务器

肯定的“需要”结果表示，自客户端计算机上次连接 WSUS 服务器以来，确定该更新是所需的更新，但尚未安装更新。因此，当更新的状态为“需要”时，可能存在以下情形。

- 更新已审批，但尚未将其下载或安装到计算机上。
- 已将更新下载到计算机，但尚未进行安装。
- 已下载并安装了更新，但在安装更新后客户端计算机尚未连接 WSUS 服务器。
- 已下载并安装了更新，但在更改生效之前要求重新启动客户端计算机，而客户端计算机尚未重新启动。

9.6　项目完成结论

WSUS 对于较大的单位来说还是非常有必要的。一方面可节约流量，减小网络压力；另一方面，先在少数计算机上测试后再在同类计算机上安装微软更新，对于公司的系统安全也有益处。

部署 WSUS 要使用组策略，这样才能快速方便。对于小公司，也可以使用自动审批。

9.7　练习案例

某公司有 1 000 台计算机，使用微软的操作系统，有 Windows XP、Windows Server 2003、Windows Server 2008 和 Windows 7 等。办公软件使用的也是 Windows 的 Office 系列产品，包括 Office 2003 和 Office 2007 等。该公司准备使用 WSUS 对公司内计算机进行更新维护。公司工作时间业务繁忙，夜晚为了节约电能，大部分计算机要关机，更新时间最好设置在午饭时间。为了保证系统安全，要求必须经过小范围测试后才能大面积更新。请你为该公司设计部署方案。

9.8　课后习题

1．公司为什么要使用 WSUS 服务？
2．为什么要对更新进行审批？如何审批？
3．为什么要建立计算机组？
4．简述 WSUS 服务器和客户端配置的过程。
5．在完成本章的各个练习的过程中，你遇到了哪些问题？是怎么解决的？

项目 10　综合项目实践：企业内部网络设计实践

本项目重点归纳在本教材中前 9 章所讲述的服务器角色的使用，并通过一个完整的案例，将本教材的全部内容整合在一起，要求学生根据要求独立完成企业网络服务系统的建设过程，掌握企业需求是如何总结的，掌握企业网络服务系统需求分析的过程和设计的详细过程，还要求学生能够在企业网络项目实施之前针对企业网络项目给出测试方案。本项目并没有给出项目的实际完成过程，而是详细描述了企业网络建设的要求，并详尽分析了该项目的需求，针对需求提供了解决方案。学生应该能够根据项目的需求及详细解决方案，参照前 9 章项目的内容独立完成整个项目的实施过程和测试过程。

知识点、技能点

- 掌握网络需求分析的方法
- 掌握网络综合设计的要素
- 掌握多种常用服务器在网络基础设施中的作用
- 掌握网络设计的原则

10.1　工作场景描述

DHYNET 公司是一家国内知名的民营企业，拥有近万名员工，产业涉及房地产、教育、外贸、休闲广场、烟草等多种行业，公司有近 10 000 台运行 Windows Server 2008、Windows Server 2003、Windows XP Professional 和 Windows 7 的计算机。公司总部位于宁波，并分别在北京、上海设有分公司。总部设有房地产、外贸、烟草和教育 4 个部门，每个分公司都由销售、财务、教育 3 个部门组成，由总部统一管理。

DHYNET 公司的组织架构如图 10-1 所示。

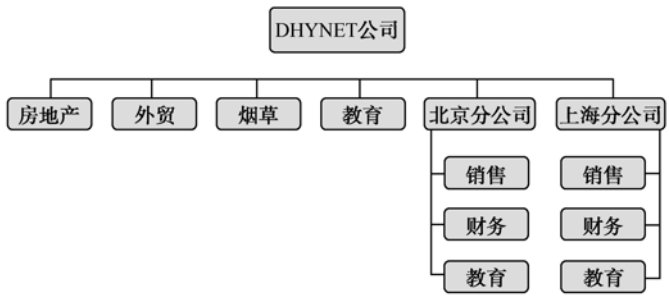

图 10-1　DHYNET 公司的组织架构

DHYNET 公司经过前期的准备，已经完成了网络组网阶段的全部工作，该公司目前全部采用了基于 CISCO 公司的交换机、路由器、防火墙。完成了网络架构的设计和施工工作，现在需要完成企业网络服务的设计、架设和实施工作。通过对该公司企业网络服务功能的设计及实施，要求在全 DHYNET 公司范围内实现 DNS、DHCP、Web、FTP、邮件、证书、WSUS 系统更新服务及远程管理等系统服务。

10.1.1　企业网络项目需求

该公司要求在企业网络设备设计及实施完毕后，为企业网络系统添加必要的 DNS 服务、DHCP 服务、VPN 服务等，并要求实现 Internet 用户访问公司 Web 和 FTP 站点，同时要求该公司能够利用 VPN 技术实现分公司和总公司的安全数据通信。

1．网络服务器设计总体需求

本项目的实施目标如下。

- 本项目要求最终为 DHYNET 公司建立一个服务齐全，满足公司办公要求，能够为该公司提升企业办公效率的高效、稳定、可靠、可扩展的高信息化办公网络。
- 所有员工都能享受到公司的信息化办公环境。
- 为公司建立公司的门户网站及应用系统网站。
- 为公司建立 DHCP 服务器，以满足部分网络的客户端计算机可以自动获得 IP 地址及必要的 TCP/IP 信息的要求。
- 为公司建立 DNS 服务器，使公司内部的 OA 系统、财务系统及其他应用系统可以使用方便的 FQDN 名称来进行访问。
- 为公司建立 VPN 服务器，使公司员工出差在外，也能使用 VPN 接入到公司内部，以访问公司内部的 OA 系统及其他内部服务系统。
- 为公司建立远程访问服务器，使公司管理员能够通过网络管理软件远程控制及管理公司内部的重要服务器。
- 为公司建立证书服务器，以满足对部分 Web 站点的安全访问及部分文件服务器的安全信息传输。
- 为公司建立 WSUS 服务器，为公司重要的服务器及 PC 提供系统自动更新服务。
- 为了实现公司的统一管理，全公司要求采用基于 Windows 活动目录管理机制来完成管理。

2．系统结构需求

随着公司近年来的飞速发展，公司时刻在扩展公司的主营业务，从最早的烟草行业起步，逐步涉及到房地产、休闲服饰广场、饮用水、教育、药业。随着公司的发展，公司内部组织结构也日益复杂。该公司要求，在设计公司企业网络的同时，要充分考虑到公司日后的扩展性、整合性，要尽量避免公司资源的浪费，要最大效能地发挥公司的信息化网络环境。要求为该公司设计合理的服务系统架构，并能满足公司的各项要求。

具体的设计应依据以下原则。

1）技术先进性

计算机网络技术的发展非常迅速，在计算机应用领域占有越来越重要的地位。必须认识到，建立计算机网络是一个动态的过程，在这个过程中将不断有新技术产生，有新产品出现。因此，一定要采用最先进的组网技术，选用代表当今世界潮流趋势的计算机公司的网络产品，才能在未来的发展中保持技术领先。

2）国际标准及开放性

现代网络技术的发展趋势是遵循国际统一标准的开放系统、支持分布式计算和客户-服务器模式，能运行多种网络操作系统、网络协议，可兼容其他厂商的网络产品。这样，才能在未来的发展中保持网络配置和应用模式的灵活性。

3）充足的、可扩展的带宽

随着应用软件复杂程度的增加、网络用户数量的增长，以及多媒体技术的普及，当今网络对带宽的需求日益增加。传统的共享式 10M/16M 网络已不能满足需求。网络系统应该能为用户提供足够的带宽，满足用户的实际应用需求，并且带宽应该是动态可调整、可扩展的。

4）安全可靠性

网络的安全可靠性是网络的一个重要的指标。计算机网络系统必须绝对可靠，网络设计必须重点考虑可靠性。从结构设计、产品选择，以及网络管理上要对网络的可靠性做出保证。安全性与可靠性同样重要，除了系统提供多种安全控制的手段外，网络设计也要提供保障其安全的手段。

5）可管理性

网络是一条信息公路，设计时必须提供足够的手段对信息公路进行方便的管理，以确保其始终保持在最佳状态下运行。没有网络管理功能将很难保证系统的正常运行。

6）实用性

网络设计一定要充分保护网络系统现有的资源。同时要根据实际情况，采用新技术和新装备，还需要考虑组网过程要与平台建设及开发同步进行，建立一个实用的网络。力求使网络既满足目前需要，又能适应未来发展，同时达到较好的性价比。

3．操作系统的选择需求

由于公司部门繁杂、人员众多、发展迅速，导致无法统一操作系统，为了满足公司管理的需求，要求允许多种操作系统共存，但是为了管理的方便，要求个人计算机（含笔记本电脑）必须安装同一公司的产品，产品的版本可以在一定的控制范围之内，且要求操作系统采用当前市场份额较大的、较为先进的操作系统；网络中的各主要服务器应视需要尽量选择应用简单、使用范围广、便于维护及管理的操作系统，特殊服务器群组的操作系统另做打算。

操作系统选型应依据如下原则。

（1）客户端操作系统要求要考虑版本和适用范围，在此基础上尽量选择最新版本。

（2）所选择的客户端操作系统不应该花费公司大量的培训时间，应能使公司用户更快上手使用。

（3）客户端操作系统应能够满足公司整体的安全需求。

（4）应尽可能选择主流厂商，要考虑及时的技术支持。

（5）服务器端操作系统如无特殊需求，应采用最新版本或最稳定版本。

（6）服务器端操作系统应能够集成 DHCP、DNS、Web、FTP、VPN、远程终端、系统更新服务，不应该再花费额外的费用购置第三方软件服务。

（7）服务器端产品视需求可以采用第三方开源操作系统，但是不应该增加公司的培训费用。

（8）服务器端操作系统应能够提供较好的安全管理策略。

（9）服务器端操作系统必须能够提供目录服务的功能，便于公司进行统一的安全策略管理、集中管理。

（10）服务器端操作系统应有足够的应用能力，以满足公司日益发展的需要，应考虑公司的长远发展，并能预留一定的访问能力。

4．活动目录服务器需求

由于公司人员众多、机构繁杂，要求能够尽可能地提供一种集中式管理机制，要求能够灵活、方便地控制网络的使用行为，能够针对不同的用户做出不同的策略，能够实现统一的安全规划。

5．DHCP 服务器需求

由于公司有多个车间，且各个车间的计算机数据较多、该部门 IT 管理人员水品较低、员工计算机水平有限，因此需要能够根据公司的实际情况考虑在多个部门实现静态 IP 地址及动态 IP 地址分配机制共存的要求。要求设计合理的 IP 地址分配方案，以使动态获取的 IP 地址不能同网络中已有的静态地址发生冲突。

6．DNS 服务器需求

由于公司内部存在多种应用程序服务器，为了便于员工访问，要求所有的应用程序服务器（如 OA 系统、财务系统）应该都能够采用 FQDN 的形式进行访问，且公司已经申请了域名 dhynet.com，要求各个服务器完全以二级域名的形式进行 IP 地址分配及域名注册。

7．证书服务器需求

为了便于在总公司和分公司之间进行 VPN 访问，部分 Web 站点的安全访问、部分重要文件服务器的 IPSec 访问，需要提供证书服务功能。

8．Web 服务器需求

公司是一家多业务公司，随着因特网的高速发展，要求公司的所有主营业务都采用 Web 服务的方式提供对外服务。要求为公司所有的主营业务规划和实施 Web 服务器的配置。公司的域名已经申请完毕为 dhynet.com，现要求配合 DNS 服务，实现公司内外的 Web 服务器访问。公司的主页采用 www.dhynet.com，其他的 Web 站点采用二级域名。对安全性要求较高的 Web 服务器采用实名访问、加密数据传输，对其他 Web 服务器可以开放匿名访问。

9．FTP 服务器需求

为了便于公司统一管理文件，方便员工使用公司的信息化资源，在已有文件服务器的基础上，需要建立 FTP 服务器，要求不额外购买第三方软件，简单易用，能够实现上传和下载，能够实现不同用户的分级访问。对出差在外的员工也能使用公司内部的 FTP 服务。

10．终端服务器需求

由于公司有众多的服务器，需要大量的 IT 管理人员完成公司整个信息系统的管理工作，为了方便 IT 部门员工的管理，要求所有的服务器可以使用管理工具进行远程管理，同时对于一些购买较早的客户端计算机，应能提供终端服务解决方案，以使这些客户端计算机能够运行超过自身应用能力的软件。

11．系统更新服务器需求

由于公司发展迅速，公司内部服务器、个人计算机的数量庞大，要求能够使用统一的系统更新服务，以降低 IT 管理员的工作量。

12．系统安全需求

根据防范安全攻击的安全需求、需要达到的安全目标、对应安全机制所需的安全服务等因素，参照 SSE-CMM（系统安全工程能力成熟模型）和 ISO17799（信息安全管理标准）等国际标准，综合考虑可实施性、可管理性、可扩展性、综合完备性、系统均衡性等方面的内容，网络安全防范体系在整体设计过程中应遵循以下 9 项原则。

1）网络信息安全的木桶原则

网络信息安全的木桶原则是指对信息均衡、全面地进行保护。“木桶的最大容积取决于最短的一块木板”。网络信息系统是一个复杂的计算机系统，它本身在物理上、操作上和管理上的种种漏洞构成了系统安全的脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用“最易渗透原则”，必然会在系统中最薄弱的地方进行攻击。

因此，充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测（包括模拟攻击）是设计信息安全系统的必要的前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，根本目的是提高整个系统的“安全最低点”的安全性能。

2）网络信息安全的整体性原则

要求在网络发生被攻击、被破坏等事件的情况下，必须尽可能地快速恢复网络信息中心的服务，减少损失。因此，信息安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全威胁采取的相应的防护措施，以避免非法攻击的进行。安全检测机制是检测系统的运行情况，及时发现和制止对系统进行的各种攻击。安全恢复机制是在安全防护机制失效的情况下，进行应急处理，并尽量、及时地恢复信息，以减少攻击的破坏程度。

3）安全性评价与平衡原则

对任何网络来说，绝对安全都难以达到，也不一定是必要的，所以需要建立合理的实用安全性和用户需求评价与平衡体系。安全体系设计要正确处理需求、风险与代价的关系，做到安全性与可用性相容，做到组织上可执行。评价信息是否安全，没有绝对的评判标准和衡量指标，只能决定于系统的用户需求和具体的应用环境，具体取决于系统的规模和范围，系统的性质和信息的重要程度。

4）标准化与一致性原则

系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，这样才能确保各个分系统的一致性，使整个系统安全地互连互通、信息共享。

5）技术与管理相结合原则

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育和安全规章制度建设相结合。

6）统筹规划，分步实施原则

由于政策规定、服务需求的不明朗，环境、条件、时间的变化，攻击手段的进步，安全防护不可能一步到位。可在一个比较全面的安全规划下，根据网络的实际需要，先建立基本的安全体系，保证基本的、必须的安全性。但随着今后网络规模的扩大和应用的增加，以及网络应用和复杂程度的变化，网络脆弱性也会不断增加，这时就要调整或增强安全防护力度，保证整个网络最根本的安全需求。

7）等级性原则

等级性原则指的是安全层次和安全级别。良好的信息安全系统必然是要分为不同等级的，包括对信息保密程度分级、对用户操作权限分级、对网络安全程度分级（安全子网和安全区域）、对系统实现结构分级（应用层、网络层、链路层等），从而针对不同级别的安全对象，提供全面、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

8）动态发展原则

要根据网络安全的变化不断调整安全措施，适应新的网络环境，满足新的网络安全需求。

9）易操作性原则

首先，安全措施需要人为去完成，若措施过于复杂，对人的要求过高，则本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

13．硬件需求

在公司网络服务系统升级改造的同时，公司投入资金，对目前配置较低、年代久远、不适合目前工作需要的计算机进行了更新，同时也给一些部门添置了新计算机，并要求计算机或服务器全部为大厂稳定产品，所有客户端计算机要求预装正版操作系统。所有服务器产品应能适合公司的整体建设需求，满足公司所需服务器的各项条件。在保障质量的同时要有最低的成本。

10.1.2　工程实施与验收

本网络项目自合同生效之日开始，要求在 30 天之内完成网络服务的系统建设。项目施工完毕，由公司及项目实施单位共同验收。工程实施单位在进行项目投标时应附带较为详细的工程实施与验收标准，我公司技术人员将根据工程实施单位提供的验收标准进行审定，提出修改意见，最后由公司 IT 项目经理、IT 工程师及工程实施单位的测试工程师、技术人员一起组成验收小组，对本公司提出的各项需求进行逐一的验收校验。

在项目验收之前，工程实施单位应提供全部网络服务系统的建设方案，以及各个服务器的详细配置手册。

验收测试完毕，工程实施单位应提供所有本网络服务建设项目的最终文档，包括技术资料。如不能通过验收，工程实施单位应给出补救方案。如不能提供完备的项目实施文档，本公司有权拒绝认定项目完成。

10.1.3　售后服务支持

在本工程通过验收后，工程实施单位必须提供至少 3 个月的 24 小时上门服务，并提供 3 年的技术支持。对于在 1 年内反复出现的故障问题，由工程实施单位负责重新制定方案并重新施工。

工程实施单位应主动联系各硬件厂商及软件厂商为我公司提供 1 年及以上的免费软件更新及硬件维护支持。1 年之内工程实施单位应将全部软、硬件厂商的服务资源逐步过渡到本公司的 IT 管理部门。

在 3 个月内出现的故障问题，应在我公司提出故障维护需求 5 小时内到达现场，并在 10 小时内提出替代方案，24 小时内解决问题。对重要服务器应在最短时间内予以解决。

在本工程项目通过验收后，工程施工单位应在一周内提供免费的技术培训计划，要求对我公司 IT 管理部门的员工进行相应的业务培训，要求培训人员应获得厂商的职业资格认证。例如，若采用 Windows 网络服务系统，则应指派具备 MCT 资格的人员进行培训；若采用 Linux 网络服务系统，则应指派具备 RHCE 资格的人员进行培训。培训的内容应包含网络服务的架设过程、故障排除、性能优化、常用的设置等。

对操作系统界面的培训由本公司 IT 管理部门完成。由工程实施单位协助完成。

由工程实施单位负责为我公司培养至少两名具备职业资格认证的人员。

培训费用由工程实施单位承担，场地由本公司负责。

10.2　网络服务系统方案设计

10.2.1　网络系统建设目标

根据 DHYNET 公司的网络服务系统设计要求，可为该公司建立如下设计方案。

全部方案以实现 DHYNET 公司高效、可靠、稳定、安全的信息化建设为主要目标，按照该公司的需求，分模块完成该公司的网络系统建设。

- 整体方案设计。
- 网络服务器配置计划（DNS、FTP、DHCP 等）。

根据 DHYNET 公司对网络服务系统的具体要求，在满足该公司所有网络应用目的的基础上，考虑该公司的最佳兼容性，排除特殊服务器群组的应用建设，为该公司规划了如下软件。

1．服务器操作系统

针对目前服务器操作系统产品情况，主要考虑 Windows 系列、Linux 系列和 UNIX 系列 3 种产品。为了满足公司简单、易用、良好的技术支持及售后服务原则，最终决定采用微软公司的 Windows Server 2008 系列产品。

2．客户端操作系统

考虑到目前 Windows 系列产品的广泛占有率，以及普及的图形化界面管理环境，在客户端操作系统上，选择了微软公司的 Windows XP Professional 产品及 Windows 7 系列产品（视计算机的硬件性能决定使用 Windows 7 还是 Windows XP 产品）。

3．网络服务器软件

DHYNET 公司所需服务分为集中式管理功能、DNS 服务功能、DHCP 服务功能等，这些服务完全集成在 Windows Server 2008 操作系统中，不需额外花费购置费用。且由于采用同一公司的产品，在最大限度上保证了系统的兼容性。

本系统在充分考虑 DHYNET 公司需求的基础上，提供了良好的建设方案，在保证用户需求的基础上，最大程度地降低了项目成本。

10.2.2　总体设计思想

从长远的角度看，计算机将决定人类的生活方式，同时网络的出现，也必将影响着一个公司的整体运营机制，可以说计算机网络的发展，不仅提高了企业的工作效率，也带来了企业信息化管理的革命式发展。随着网络产品的发展，企业网络应用的需求不断扩大，信息化建设不断出现新的技术及解决方案。现近流行的虚拟化技术、云计算技术无一不是瞄准了信息化建设这块巨大的商业蛋糕。在充分考虑 DHYNET 公司的网络服务系统需求的基础上，我们提供了如下的系统总体设计方案思想。

网络设计要解决的主要是 4 个问题，即选择什么样的网络技术，选择什么样的厂商，选择什么样的产品，选择什么样的方案配置。那么根据什么原则来确定这些问题的答案呢？

1．开放性原则

随着开放互连标准的规定，只有开放的、符合国际标准的网络系统才能够实现多厂家产品的互连。

2．可扩充性原则

网络系统要灵活地扩充，可扩充对网络而言有两方面的内容。第一是能够适应网络规模的扩充，第二是能够适应应用提升对系统性能的更高要求。具有良好扩充性的网络系统能够让用户以较小的代价扩充现有网络服务的功能，这样，就有效地保护了用户的投资。

3．可靠性原则

用户的网络系统必须具有一定的容错能力，保障在意外情况下不中断用户的正常工作。可靠性也是通过设备可靠性和技术措施两个层次的方式来解决的。首先，要求所选择的网络厂商

产品性能要稳定可靠；其次，要求网络厂商有充足的备件，在网络服务发生故障后能够得到及时更换；第三，通过技术措施来保证网络的可靠性，如采取重要服务器集群技术，采用部件冗余技术，采用链路通道技术等。通过这些措施使得网络即使出现某些故障仍然能够正常运行。

4．可管理性原则

网络系统应该能够支持 SNMP（简单网管协议）和 RMON，这样便于计算机管理人员通过网管软件随时监视网络的运行状况。一旦出现故障，系统可以自动报告出错位置和出错原因，管理人员可以迅速发现故障并及时维护。同时 SNMP V2 版本的协议还支持很多更高级的网络安全管理功能。

网络的可管理性对整个系统具有至关重要的意义。现在网络和应用变得愈来愈复杂，一个不可管理的网络是不可想象的。

5．先进性和实用性原则

先进性和实用性是相辅相成的，网络技术和产品的先进性保证了系统的高性能，实用性保证了网络的高效率。现在各种新技术和应用层出不穷，但经过一段时间的大浪淘沙后，只有少数技术才能成为真正的主流。影响新技术前途的关键因素之一，是新技术与现有技术和设备的兼容性。所以选择原则有两条：一是新技术能够和已有技术无缝集成；二是新技术适合用户的应用场合。只有先进的且适合于用户应用的技术才是正确的选择。

6．选择占主导地位的厂家，保护用户投资

网络是用户信息系统的中枢神经。随着用户企业规模的发展，用户的网络系统也要不断扩展、不断升级。占主导地位的网络厂家的优势在于：

- 产品市场占有率高，广泛的用户群可以支持厂家良好经营，不断发展；
- 拥有最先进的技术，使其产品不断升级，通过产品升级一方面使其用户得到最先进的技术，另一方面可以保护用户以前的设备投资。

10.2.3　系统架构设计

根据公司的集中式管理需求、统一的安全策略需要，在本项目中采用了 Windows 系统中最为核心的技术-活动目录域管理模式。使用基于 Windows 的活动目录机制主要由以下几个方面的优势。

1．信息的安全性大大增强

安装活动目录后信息的安全性完全与活动目录集成，用户授权管理和目录进入控制已经整合在活动目录当中了（包括用户的访问和登录权限等），而它们都是 Windows Server 2008 操作系统的关键安全措施。活动目录集中控制用户授权，目录进入控制不仅能在每一个目录中的对象上定义，而且还能在每一个对象的每个属性上定义，这一点是以前任何系统所不能达到的。除此之外，活动目录还可以提供存储和应用程序作用域的安全策略，提供安全策略的存储和应用范围。安全策略可包含账户信息，如域范围内的密码限制或对特定域资源的访问权限等。所以从一定程度上可以这么说，Windows 的安全性就是活动目录所体现的安全性，由此可见对于网络管理人员来说如何配置好活动目录中对象及属性的安全性是管好 Windows Server 2008 系统的关键。

2．引入基于策略的管理，使系统的管理更加明朗

活动目录服务包括目录对象数据存储和逻辑分层结构（指上面所讲的目录、目录树、域、域树、域林等所组成的层次结构）。作为目录，它存储着分配给特定环境的策略，称为组策略

对象。作为逻辑结构，它为策略应用程序提供分层的环境。组策略对象表示了一套商务规则，它包括与要应用的环境有关的设置，组策略是用户或计算机初始化时用到的配置设置。所有的组策略设置都包含在应用到活动目录、域或组织单元的组策略对象（GPOs）中。GPOs 设置决定目录对象和域资源的进入权限，什么样的域资源可以被用户使用，以及这些域资源怎样使用等。例如，组策略对象可以决定当用户登录时用户在它们的计算机上能看到什么应用程序，当它在服务器上启动时有多少用户可连接至 Server，以及当用户转移到不同的部门或组时它们可访问什么文件或服务。组策略对象使您可以管理少量的策略而不是大量的用户和计算机。通过活动目录，您可将组策略设置应用于适当的环境中，不管它是您的整个单位，还是您单位中的特定部门。

3．具有很强的可扩展性

Windows Server 2008 的活动目录具有很强的可扩展性，管理员可以在计划中增加新的对象类，或者给现有的对象类增加新的属性。计划包括可以存储在目录中的每一个对象类的定义和对象类的属性。例如，在电子商务上你可以给每一个用户对象增加一个购物授权属性，然后存储每一个用户购买权限作为用户账号的一部分。

4．具有很强的可伸缩性

活动目录可包含在一个或多个域中，每个域具有一个或多个域控制器，以便您可以调整目录的规模，从而满足任何网络的需要。多个域可组成域树，多个域树又可组成树林，活动目录也就随着域的伸缩而伸缩，较好地适应了单位网络的变化。目录将其架构和配置信息分发给目录中所有的域控制器，该信息存储在域的第一个域控制器中，并且复制到域中任何其他的域控制器。当该目录配置为单个域时，添加域控制器将改变目录的规模，而不影响其他域的管理开销。将域添加到目录使您可以针对不同策略环境划分目录，并调整目录的规模以容纳大量的资源和对象。

5．智能的信息复制能力

信息复制为目录提供了信息可用性、容错、负载平衡和性能优势，活动目录使用多主机复制，允许您在任何域控制器上而不是单个主域控制器上同步更新目录。多主机模式具有更大容错的优点，因为使用多域控制器，即使任何单独的域控制器停止工作，也可继续复制。由于进行了多主机复制，它们将更新目录的单个副本，在域控制器上创建或修改目录信息后，新创建或更改的信息将发送到域中的所有其他域控制器，所以其目录信息是最新的。域控制器需要最新的目录信息，但是要做到高效率，必须把自身的更新限制在只有新建或更改目录信息的时候，以免在网络高峰期进行同步而影响网络速度。在域控制器之间不加选择地交换目录信息能够迅速搞垮任何网络。通过活动目录就能达到只复制更改的目录信息的目的，而不至于大量增加域控制器的负荷。

6．与 DNS 集成紧密

活动目录使用域名系统（DNS）来为服务器目录命名，DNS 是将更容易理解的主机名（如 Mike.Mycompany.com）转换为数字 IP 地址的 Internet 标准服务，利于在 TCP/IP 网络中计算机之间的相互识别和通信。DNS 的域名基于 DNS 分层命名结构，这是一种倒置的树状结构，单个根域在它下面可以是父域和子域（分支和叶子）。

7．与其他目录服务具有相互操作性

由于活动目录是基于标准的目录访问协议的，许多应用程序界面（API）都允许开发者进入这些协议，如活动目录服务界面（ADSI）、轻型目录访问协议（LDAP）第三版和名称服务

提供程序接口（NSPI），因此它可与使用这些协议的其他目录服务相互操作。LDAP 是用于在活动目录中查询和检索信息的目录访问协议。因为它是一种工业标准服务协议，所以可使用 LDAP 开发程序，与同时支持 LDAP 的其他目录服务共享活动目录信息。活动目录支持 Microsoft Exchange 4.0 和 5.x 客户程序所用的 NSPI 协议，以提供与 Exchange 目录的兼容性。

8．具有灵活的查询

任何用户可使用“开始”菜单、“网上邻居”或“活动目录用户和计算机”上的“搜索”命令，通过对象属性快速查找网络上的对象。例如，可通过名字、姓氏、电子邮件名、办公室位置或用户账户的其他属性来查找用户，反之亦然。

由于 DHYNET 公司的分公司全部为独立核算、自主经营，这种独特的管理模式虽然促进了该公司的业务发展，但是给网络建设提出了较高的难度。为此我们为该公司设计了多域的管理模式，在总公司设计父域，在各个分公司采用子域的管理模式，一方面考虑到涉及广域网的复制流量，一方面也能降低管理开销。

10.2.4　网络服务系统设计

IP 地址规划设计

根据公司的实际情况，设计该公司服务器 IP 地址范围为 10.0.0.0/24，各部门的 IP 地址按照 10.0.1.0/24……10.0.2.0/24 划分。

北京分公司使用的 IP 地址范围从 10.1.0.0/24 开始，按照 10.2.0.0/24……10.3.0.0/24 的方式递增。

上海分公司使用的 IP 地址范围从 10.10.0.0/24 开始，按照 10.10.0.0/24……10.11.0.0/24 的方式递增。

各服务器的 IP 地址配置如表 10-1 所示。

表 10-1　服务器角色与 IP 地址映射表

服务器角色	IP 地址
DC	10.0.0.1
CA	10.0.0.2
SMS	10.0.0.3
DHCP	10.0.0.4
FTP	10.0.0.5
WSUS	10.0.0.6
WWW	10.0.0.7
额外 DC	10.0.0.10
北京子域 DC	10.1.0.1
北京子域额外 DC	10.10.0.1
各网段网关	网段+.254 结尾

10.2.5　网络服务拓扑设计

DHYNET 公司网络服务系统拓扑图如图 10-2 所示。

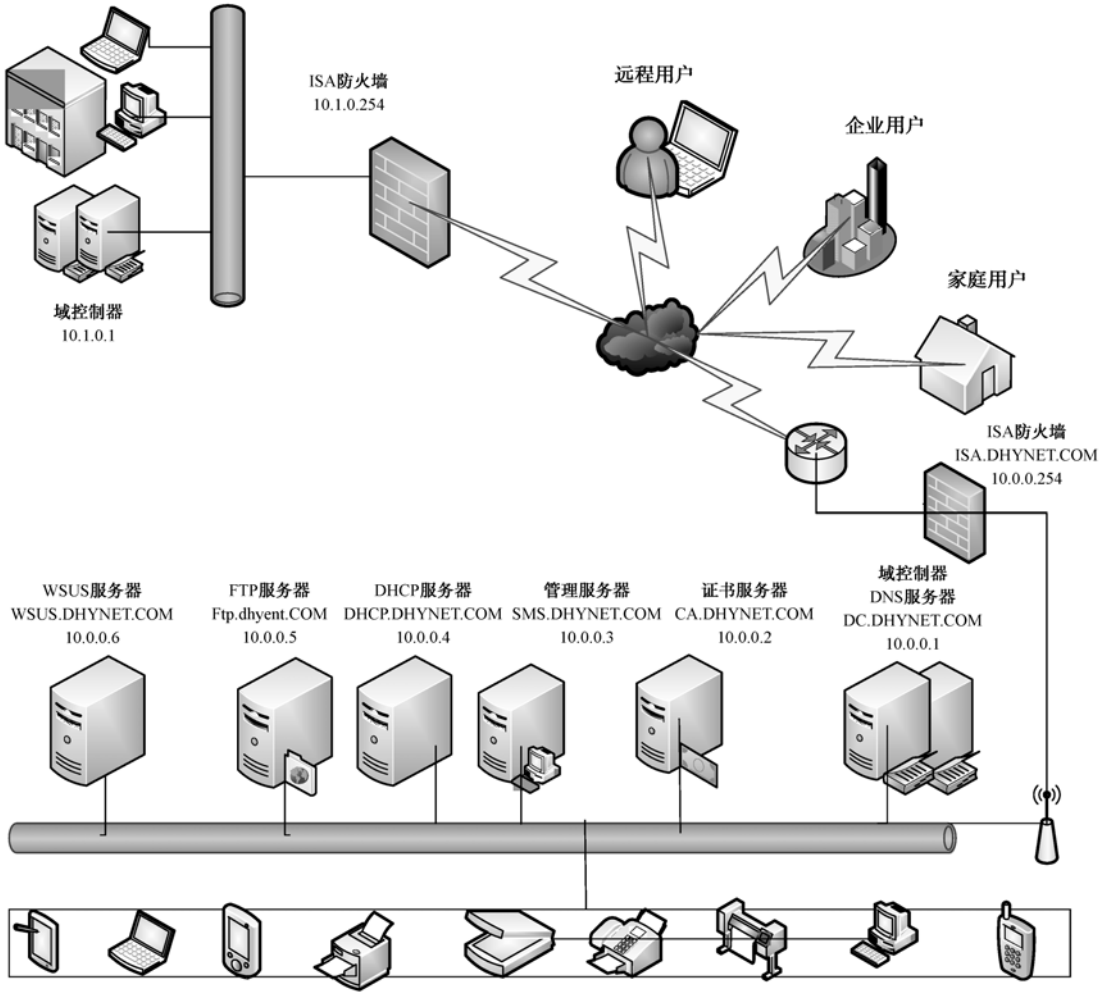

图 10-2　DHYNET 公司网络服务器部署图

10.2.6　活动目录结构设计

DHYNET 公司活动目录结构设计如图 10-3 所示。

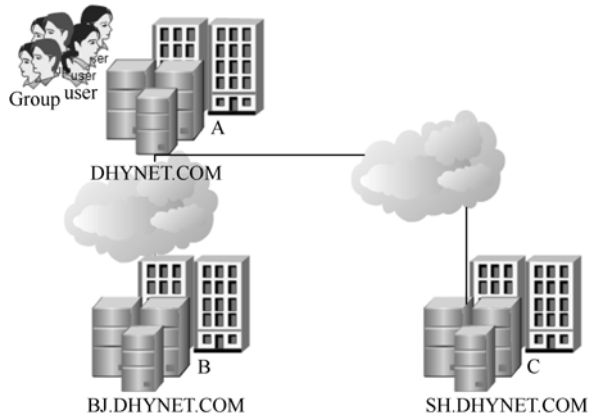

图 10-3　DHYNET 公司活动目录结构部署图

10.2.7　DHCP 角色服务的设计

根据公司的需求，在公司的生产车间、部分办公区域采用了动态 IP 地址的设计方案，满足了降低网络管理的需要。

DHCP 服务器的具体配置如表 10-2 所示。

表 10-2　DHCP 服务器配置

配　　置	配　置　值
位置	公司总部 DHCP 服务器
服务器名	Dhcp
IP 地址	10.0.0.4/24
端口	67/68
域名	Dhcp.dhynet.com
管理者	IT mana group
服务器品牌	联想
使用范围	总公司内部
备用/主要	主要
主要配置	租约：8 天 作用域 1：10.0.1.0/24 路由器：10.0.1.254 作用域 2：10.0.2.0/24 路由器：10.0.2.254 作用域 3：10.0.3.0/24 路由器：10.0.2.254 DNS Addres：10.0.0.1

10.2.8　AD 域角色服务的设计

根据公司的需求，为了实现集中式管理、安全管理，降低管理成本，采用基于活动目录域的管理模式。

AD 域角色服务器的具体配置如表 10-3 所示。

表 10-3　AD 服务器配置

配　　置	配　置　值
位置	公司总部 AD 服务器
服务器名	Ad
IP 地址	10.0.0.1/24
端口	88/389
域名	ad.dhynet.com
管理者	IT mana group

续表

配　　置	配　置　值
服务器品牌	联想
使用范围	总公司内部
备用/主要	主要
主要配置	新域→新树→新森林 域名：ad.dhynet.com 管理密码：P@ssw0rd 目录恢复模式密码：Pa$$w0rd 操作主机：架构主机角色、域命名主机角色、RID 主机角色、PDC 模拟器主机角色、基础结构主机角色、全局编录服务器 NTFS 分区
备注	有额外域控制器 子域 1：bj.dhynet.com→10.1.0.2 子域 2：sh.dhynet.com→10.10.0.2

10.2.9　DNS 角色服务的设计

根据公司项目需求，为了便捷地访问各 Web 服务器，使用基于 FQDN 的方便记忆的名字来实现域名到 IP 地址的映射，为该公司配置 DNS 服务器。

DNS 服务器的具体配置如表 10-4 所示。

表 10-4　DNS 服务器配置

配　　置	配　置　值
位置	公司总部 DNS 服务器
服务器名	Ad
IP 地址	10.0.0.1/24
端口	53
域名	ad.dhynet.com
管理者	IT mana group
服务器品牌	联想
使用范围	总公司内部
备用/主要	主要
主要配置	主要区域：dhynet.com 与活动目录集成区域 主机记录采用动态注册 对应服务器的 FQDN 与 IP 映射关系 Ad.dhynet.com：10.0.0.1 Dhcp.dhynet.com：10.0.0.4 www.dhyent.com：10.0.0.7

续表

配　　置	配　置　值
主要配置	ftp.dhynet.com：10.0.0.5 ca.dhynet.com：10.0.0.2 wsus.dhynet.com：10.0.0.6 sms.dhynet.com：10.0.0.3 建立相应的反向区域 设置转发器 bj.dhynet.com 转发 10.1.0.2 sh.dhynet.com 转发 10.10.0.2 其他转发到 8.8.8.8
备注	与 AD 域角色服务器集成

10.2.10　Web 角色服务的设计

根据公司的需求，在公司内部配置一台 Web 服务器，设置相应的站点。Web 服务器的具体配置如表 10-5 所示。

表 10-5　Web 服务器配置

配　　置	配　置　值
位置	公司总部 Web 服务器
服务器名	www
IP 地址	10.0.0.7/24
端口	80
域名	www.dhynet.com
管理者	IT mana group
服务器品牌	联想
使用范围	总公司内部
备用/主要	主要
主要配置	主页：dhynet.aspx 主目录：d:\www 权限：读写、执行 端口：80 建立主机头访问 1：oa.dhynet.com IP 地址为 10.0.0.7 主目录为：d:\oa 主页为：oa.aspx 权限：读写、执行 建立主机头访问 2：ex.dhynet.com IP 地址为 10.0.0.7

续表

配　　置	配　置　值
主要配置	主目录为：d:\ex 主页为：ex.aspx 权限：读写、执行 访问设置：实名访问 建立主机头访问 3：file.dhynet.com IP 地址为 10.0.0.7 主目录为：d:\file 主页为：file.aspx 权限：读写、执行 访问设置：采用加密数据传输，要求证书 端口：443 密钥长度：128 位
备注	有公网地址采用 NAT 映射

10.2.11　CA 角色服务的设计

CA 服务器为网络提供身份验证及加密解密的证书服务，为安全的 Web 服务器提供加密数据传输及身份验证机制，为 IPSec 提供加密信道中所有的密钥服务。

CA 服务器的具体配置如表 10-6 所示。

表 10-6　CA 服务器配置

配　　置	配　置　值
位置	公司总部 CA 服务器
服务器名	CA
IP 地址	10.0.0.2/24
域名	ca.dhynet.com
管理者	IT mana group
服务器品牌	联想
使用范围	总公司内部
主要配置	企业根 证书名：dhynet 有效期：5 年 集成 Web 7.0 虚拟目录：certsrv

10.2.12　FTP 角色服务的设计

根据用户的需求分析，为便于实现公司内部信息的高效使用，建立 FTP 服务器。

FTP 服务器的具体配置如表 10-7 所示。

表 10-7　FTP 服务器配置

配　　置	配　置　值
位置	公司总部 FTP 服务器
服务器名	ftp
IP 地址	10.0.0.5/24
端口	20/21
域名	ftp.dhynet.com
管理者	IT mana group
服务器品牌	联想
使用范围	总公司内部
主要配置	主目录：e:\ftp 权限：下载 实现账户隔离 不允许匿名访问 流量不限 用户不限 个别用户开放上传权限 有公有用 ftp 目录 发布到因特网
备注	有公网 IP 地址采用 NAT 技术映射

10.3　网络服务系统项目测试规划

网络服务系统的测试分为以下几个部分进行。

（1）网络连通性测试。

（2）各个服务功能性测试。

（3）可靠性测试。

（4）压力测试。

10.3.1　网络连通性测试

在网络中的任意一台主机上进行 ping、tracert 的测试，查看连通性及 ttl 值。

（1）Ping ad.dhynet.com 能够 ping 通。

（2）Ping ftp.dhynet.com 能够 ping 通。

（3）Ping www.dhynet.com 能够 ping 通。

（4）Ping wsus.dhynet.com 能够 ping 通。

（5）Ping sms.dhynet.com 能够 ping 通。

（6）Ping dhcp.dhynet.com 能够 ping 通。

（7）Ping ca.dhynet.com 能够 ping 通。

（8）进行跟踪测试，返回正确的响应。

10.3.2　服务器功能性测试

1．Ad 服务器角色功能测试

查看活动目录数据库文件。

查看管理工具是否出现活动目录的管理工具。

查看 DNS 服务器是否出现正确的 SRV 记录。

2．CA 服务器角色功能测试

在客户端计算机申请证书，是否能够正确申请证书。

证书服务器是否能够正常启动、暂停和停止。

证书服务器是否正确安装了 Web 服务，是否有相应的虚拟目录。

3．SMS 服务器角色功能测试

是否能够为客户端计算机提供远程访问服务器功能。

4．DHCP 服务器角色功能测试

是否能够为客户端计算机分配合适的 IP 地址、DNS 地址和网关地址。

各动态获取 IP 地址的计算机是否能够正确接入网络。

各动态获取 IP 地址的计算机是否有 IP 地址冲突情况发生。

5．FTP 服务器角色功能测试

是否能够进行匿名访问。

是否能够上传和下载。

是否实现了用户隔离。

6．WSUS 服务器角色功能测试

是否实现了服务器和客户端计算机的系统更新服务。

7．WWW 服务器角色功能测试

是否实现了 DHYNET 公司的主页访问。

是否实现了使用主机头访问 OA、EX、FILE 三个站点。

是否实现了加密传输功能。

是否实现了实名网站访问功能。

10.4　项 目 总 结

学习网络服务系统的项目设计和实施，目的是总结和归纳本教材中的重点内容，熟悉各网络角色服务在实际项目中的设计和实施过程，了解大中型企业网的构成和特点，巩固学习中的知识和技能。

学生在学习完网络角色服务系统的设计之后，可以利用常用的网络服务角色为企业的信息化建设提供自己的建议和意见，能够根据企业的实际需求选择合适的服务角色。

网络的安全设计和管理永远是企业信息化建设的重点，但是在本教材中并没有太多地涉及，原因在于网络安全防护是在网络服务系统管理、实施基础之上的应用，只有熟练掌握了企业网络服务角色的设计和实施之后，才能更好地管理企业的网络安全。

参 考 文 献

[1] 戴有炜．Windows Server 2008 网络专业指南．北京：科学出版社，2009．

[2] 刘晓辉，李利军．Windows Server 2008 安全内幕．北京：清华大学出版社，2009．

[3] Williamr Stanek．精通 Windows Server 2008．刘晖，欧阳，译．北京：清华大学出版社，2009．

[4] Orin Thomas，Paul Mancuso，John Policelli，等．Windows Server 2008 企业环境管理（MCITP 教程）．刘晖，欧阳，杨建英，译．北京：清华大学出版社，2009．

[5] Ian Mclean，Orin Thomas．Windows Server 2008 网管员自学宝典（MCITP 教程）．施平安，刘晖，张大威，译．北京：清华大学出版社，2009．

[6] Mackin，Anil Desai．Windows Server 2008 应用程序基础架构（MCTS 教程）．许华杰，孙晓刚，译．北京：清华大学出版社，2010．

[7] www.sharecenter.net．

[8] www.winos.cn．

[9] www.microsoft.com．

[10] www.51cto.com．

[11] www.chinaitlab.com．

[12] www.netadmin.com．